NERC GridSecCon 2013

October 15-17, 2013

Jacksonville, FL

[redacted] **Report**

The North American Electric Reliability Corporation (NERC) hosted the third annual Grid Security Conference (GridSecCon) on October 15-17, 2013, in Jacksonville, FL. A two-day workshop was conducted on October 15-16. Four training tracks in physical and cybersecurity took place on October 17. I attended the two-day workshop and completed CYBATI's Critical Infrastructure and Control System Cybersecurity Red/Blue Team Hands-on Exercise. The final agenda can be found by clicking on the following NERC website.
http://www.nerc.com/pa/CI/CIPOutreach/Documents/GridSecCon%202013%20Agenda%20FINAL%20(4).pdf

The theme of this year GridSecCon 2013 was about "Threats, Policy, Solutions, and the Bulk Power System". The NERC conference objectives included the following:

- Promoting reliability of the bulk power system (BPS) through training and industry education.
- Delivering cutting-edge discussions on Critical Infrastructure Protection (CIP) security threats, vulnerabilities, and lessons-learned from senior industry and government leaders.
- Informing industry with security best-practice discussions on reliability concerns, risk mitigation, and physical and cybersecurity threat awareness.

The following findings are summarized in the order of the agenda items, except as noted.

- **Welcome Address and Opening Keynote:** Mr. Gerry Cauley, President and CEO of NERC, provided welcoming remarks and **expressed that the role of government for him is to promote information sharing.** While he admitted that he had not been more engaged with "deterrence and enforcement", he believes cybersecurity is like "an addiction". As cyber attacks are relentless and bad guys are more sophisticated, therefore, Mr. Cauley believes that we (everyone working on BPS) should need to continuously share lessons learned, be "long-term adaptive", and reach a "long-term equilibrium" one day. He cited that NERC works have "risk-based priorities," the Reliability Assessment Initiative (RAI) and CIP V5 Standards are implementing "risk-based approaches" and covering "all parts of BPS one way or another." Mr. Cauley claimed that we never had a cybersecurity incident that crippled the BPS and that the ES-ISAC has been providing near real-time (same day or hour in some cases) **threats and actionable information to the electric sector members** who protect the grid. He reemphasized that there is **no sharing of compliance information between enforcement authorities and ES-ISAC**. He also mentioned the upcoming GridEx and DOE Electric Sector Cybersecurity Capability and Maturity Model (ES-C2M2) that NERC works with DOE on **a self-assessment program**. In concluding his remarks, he claimed that NERC as the ERO has formed a consortium of CEOs for setting policies and working with the Government for additional assistance.

- **Mr. Paul McElroy, CEO of Jacksonville Electric Authority (JEA),** welcomed workshop participants to Jacksonville, FL and showed his company's footprint and systems that are municipally owned. He discussed about the cybersecurity threat landscape and how NERC-ERO led the electric sector to adopt the CIP standards. He claimed that his company's focus is beyond

CIP compliance and **that mandatory standards need to evolve with risks and costs**. He said JEA needs **clarity in standards – not quantity**.

- **The Honorable Michael Chertoff, Co-Founder and Managing Principal of Chertoff Group**, talked about the "new normal" and **that risk-management and mandatory CIP standards is "a good model" for other critical infrastructure industries to follow**. **Acknowledging enhanced "accountability" in the electric sector**, he asked for more **vigilance** in cybersecurity and engagement with the government, and cited various SCADA vulnerabilities. He mentioned about an intrusion into a network thru a Wifi-connected thermostat, and said that SCADA Apps (Applications) are available everywhere now and very vulnerable. He also expressed his concerns about disgruntle employees, citing shooting at the Navy yard in Washington DC. He encouraged **critical infrastructure owners and operators to protect their core business** by employing the following: **protecting Industrial Control Systems (ICS), developing protection strategies and contingency plans, coordinating and working with CEOs; the Boards should engage and empower organizations to protect and defend critical infrastructure**. The audience asked several questions regarding how he brought all parts of DHS together; how effective today's information sharing is; current personnel assurance and clearance programs; and supply chain security. He said keeping **"mission focus"** helped DHS integrated all parts of DHS. DHS engaged **"all stake holders to have their stake in the mission"** and in the planning as well. Although there are laws in place **to protect civil liberties and privacy**, however, the world is changing, he said, and that perhaps **laws should be modified to facilitate effective, real-time information sharing.** He also expressed his concerns about supply chain security and suggested taking certain applicable features of personnel assurance, fitness, and clearance programs from the military, nuclear weapons program, and NRC. Also, he said that **every industry and vendors should comply with similar regulations, particularly standards, so that everyone can share the same load (costs) in protection** – leveling the competition.

- **Does Anyone Really Know What Time It Is? Dr. Michael Cohen** of MITRE provided a briefing concerning the vulnerabilities of GPS-clock. Dr. Cohen discussed various timing dependencies, threats, and mitigation measures, and provided some recommendations for NERC and industry consideration. The Grid is time-dependent. Phasor Measurement Unit (PMU) data, Synchrophasors network, control centers, protective relays, disturbance monitoring and measurement devices, as well as the quality of power supply and market data depend on the accuracy and reliability of the clock. The Global Positioning System (GPS) synchronizes different-time zone clocks and acts as a time setter. GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Thus, GPS is susceptible to Radio Frequency interference, space weather such **geomagnetic storms**, and vulnerable to **intentionally jamming and spoofing**. Since GPS is universally used by critical infrastructure owners and operators, it becomes a "tempting target" that **could be exploited by adversaries or groups that would cause harm to the grid infrastructure and/or to obtain economic gains.** Dr. Cohen also provided a few examples of low cost, technologies, best practices for anti-jamming and anti-spoofing. Additional research and development of emerging anti-jamming/spoofing technologies are being conducted by MITRE. In addition, he proposed to develop a GPS time and frequency system that can detect, warn of, and resist both unintentional and intentional GPS threats. In conclusion, he believes that employing multiple layers of backup capabilities, mitigation strategies and alternatives, and contingency plans to provide protection against GPS timing loss and manipulation would minimize impacts on Grid's critical infrastructure.

- **Substation Security: Lessons-Learned.** Greg Williams, security investigator of Pacific Gas and Electric Company, provided some evidence and facts regarding the MetCalf substation shooting incident on April 16, 2013. The facts revealed that the adversaries had knowledge of tactics and strategically planned for the shooting attack and their escape – First the adversaries disrupted the substation communication system (including telephone lines). Second, they positioned themselves at various locations in bushes around the substation, and fired shots at the 500/230 kV transformers that resulted in approximately $30 million worth in equipment damages. Greg Williams admitted that a Design Basis Threat did not exist for PG&E. The adversaries used knowledge of substation operations and equipment layout, tactical techniques, and assault rifles to shutdown substation operations serving the Silicone Valley, CA.

- **Afternoon Keynote Speaker - Terry Boston, CEO of PJM,** discussed about the challenges and opportunities as PJM faces a period of cybersecurity "uncertainties". Since the August 2003 Northeast/Midwest Blackout, he claimed that PJM has been in the forefront to provide better security and upgrades through collaboration and partnership with PJM members, NERC, academia, vendors, the DOE and DHS. He cited PJM program, called Cybersecurity Risk Information Sharing Program, as an example of his model of "Prevention-Collaboration-Resiliency". Without citing specific vulnerabilities, he called for greater collaboration, partnership and vigilance in facing security challenges.

- **Threat of Modern Malware – Panel Discussion:** Panelists include: Tim Roxey, Chief Cybersecurity Officer and ES-ISAC Director of NERC; Jonathan Pollet, Founder of Red Tiger Security, Mark Fabro, President and Chief Security Scientist of Lofty Perch; Billy Rios, Technical Director of Cylance. The panelists revealed trends of malware and their modes of attack. These panelists warned that modern malware might be embedded in the least expected places, like a safe haven where it cannot be detected. The malware can then spread to perform certain authenticated and authoritative commands. They may target at PMU and State Estimator's data, GPS-based system, ICCP-based protective relays. Several audience liked Mark Fabro's T-shirt that was wearing on stage. One of the phrases printed on this T-shirt said "I am in your State Estimator's Computer". They also mentioned about the recent FDA issued-Federal Register regarding the modifications (additions) of recognizable IEC, ISO, ANSI cybersecurity standards for medical devices and critical hospital networks.

- **How the Grid Will Be Hacked** – Josh Axelrod and Matt Davis, Ernst & Young, discussed about the past, present, and future state of the grid. They believed that the grid may not have experienced any devastated hacking event because of our "security thru obscurity" and the large make up of electromechanical devices on the grid. However, as the grid is modernized, lacking authentication and encryption on ICS and devices, outdated regulations and minimal security standards make the Grid an easy target for hackers. "When and where will the grid be hacked?" so one asked. The presenters said it just a matter of time and the areas that are most vulnerable were supply chain, nuclear facilities, auto manufacturers, and metal refineries. Organized cybersecurity crime is a concern in the stock market. The presenters also mentioned about the **"Seven Bullets Theory"** – one believes that a terrorist group could shut down the entire East Coast grid with just seven well-placed bullets at seven different substations. **The MetCalf substation's shooting perhaps was a miniature testing version of this theory.** In conclusion, the presenters recommended entities to stick to the fundamentals – vendors to encrypt their protocols, complied with consensus standards, security requirements, and vendors' certification with endorsement from regulators (e.g., FERC). **ES-ISAC should not only share information but perform breach analysis and share lessons learned.** Regulators or government should provide incentives for entities who comply with voluntary Cybersecurity Framework. Although,

the presenters think the self-regulated is antiquated, RAI is ok. One way to fight DDoS "is to be distributed yourself", so the presenters think micro-grid is more secure. They also believe in ISO guidance, US regulatory framework, and other international standards are needed and should be considered.

- **First Day Closing Remarks – Matt Blizard**, Director of Critical Infrastructure Protection, NERC thanked the speakers and participants and outlined NERC current strategy – That include Standard development, compliance, and enforcement, RAI, internal controls (IAC), transition from CIP V3 compliance to V5 compliance, public/private partnership as called for by EO 13636 and PPD-21, participating in the development of the National Infrastructure Protection Plan, ES-ISAC, outreach, training, and exercises (GridEx II).

- Two speakers did not attend the workshop – not sure if Government shutdown may be the reason. These two officials include **Bill Bryan**, DOE Deputy Assistant Secretary for Infrastructure Security and Energy Restoration and **Dr. Andy Ozment**, Senior Director for Cybersecurity, National Security Staff.

- **A CISSP's Perspective on CIP and Security** – Richard Kinas, Manager of Compliance, Orlando Utilities Commission, provided his views on critical infrastructure protection. He acknowledged that the CIP standards may provide the hackers targets, areas where there are not having adequate standards. In reality, some companies may have gone beyond the CIP standards. However, there are areas that he would improve upon. These include scanning ports, network vulnerabilities, watching for jump hosts, proxies; access control: understand OS vulnerabilities, buffer overflows, authentication, session hijacking, SQL injection thru authorized users; checking rootkits, backdoors and Trojans (CIP-007-5, R3); clearing system logs, remove cookies, etc…**He also acknowledged the followings were not required by CIP standards:** configuration of firewalls to perform certain defensive tasks, specific requirements for security monitoring, demonstrated needs for certain applications that may be vulnerable. **When asked if CIP standards should cover hacking methods**, he responded that it is better off to focus on risk management and mentioned that "**Honey Pots**" and/or better firewalls configuration management may provide better protection for the money spent.

- **Information Sharing Task Force Recommendations** – Stephen Diebold, Senior Director of Ventyx provided a briefing regarding the information sharing task force and its recommendations. These include:
    1. Cultivate a trusting information-sharing environment.
    2. Promote recognition of the ES-ISAC's role as the central hub for the electricity sector to share physical and cyber threat information.
    3. Reduce reporting complexity and redundancy.
    4. Implement technology to encourage unattributed information sharing.
    5. Improve information aggregation and collaborative analysis at the ES-ISAC.

- **CIP Compliance – Panel Discussion.** Panelists include Tobias Whitney, Manager of NERC CIP Compliance; Gregory Goodrich, Supervisor, Enterprise Security at New York Independent System Operator; Kevin Perry, Director of Critical Infrastructure Protection at Southwest Power Pool Regional Entity; Roger Fradenburgh, Principal Security Architect, Network & Security Technologies. The panelists answered questions concerning CIP V5transition as NERC has been planning on transitioning CIP V3 compliance to CIP V5 compliance, subject to FERC approval of CIP V5. Audience wass speculating that the Commission will approve V5 standard by the end of year and that the Identify-Assess-Correct requirements will be added later by a compliance

filing. In general, industry and panelists think CIP v5 is better than previous approved CIP standards and is one step in the right direction.

- **Electric Sector Information Sharing and Analysis Center Update** – Tim Roxey, NERC Chief Cybersecurity Officer and ES-ISAC Director, presented an update on ES-ISAC activities and the Cyber Risk Preparedness Assessment (CRPA) program. The CRPA program had six core focus areas: (1) Existing Infrastructure Security, (2) Leadership, (3) Communication, (4) Incident Response Planning, (5) Self-Organization, and (6) Operational Priorities. A table-top exercise was conducted in 2012 and its findings report was released in May 2013. http://www.esisac.com/Public%20Library/Reports/CRPA%20Program%202012%20Report.pdf. Tim Roxey mentioned that the exercise was to detect, respond, deter, and defend cyber-attacks similar to Aurora attack and may include physical (force-on-force) type of attacks in the future.

- **Outside the Box – Risk Management Solutions from Off the Shelf.** The panelists from event-sponsoring companies presented their applications and solutions to protecting critical infrastructure. Products include network traffic monitoring and risk management software that help entities to manage their assets, risks, protection mechanisms and compliance.

- **FERC Office of Energy Infrastructure Security (OEIS) –** [redacted] provided a briefing about the formation of OEIS and discussed about OEIS mission and work, including the assistance his office provided to PG&E in the investigation of the MetCalf substation attack. He said his office is working closely with ES-ISAC, planning on a classified workshop, and is Protected Critical Infrastructure Information (PCII) -certified by DHS so entities should feel comfortable in sharing PCII with his office.

- **GridEx II Success Strategy – Bill Lawrence,** NERC Manager of CIP Awareness, presented the successes of GridEx II last year and discussed on the logistics planning on the next GridEx III. He solicited industry participations and assured that they have a contingency plan in place should there is a real incident that jeopardizes the Grid. Brian Harrell, NERC Associate Director of CIP Programs concluded the 2-day GridSecCon 2013 workshop and thanked participants and speakers for staying even in the last hour.

- [redacted]ttended the training, **CYBATI Control System Security Hands-On Exercise** October 17 and received 8 CPE-Credits certificate. The day long exercise used a simulated power grid for teams to practice their hacking and defending techniques and methods. The team delegated responsibilities to protect the grid from other teams (threat actors) hacking. Real industrial controllers, communication protocols, network monitoring applications, and configuration methods and techniques were used in the exercise.

DRSS Bi-Weekly Staff Meeting, 9/11/13, 2:00 PM – 3:30 PM

[redacted]

[redacted]

[redacted]

- Physical attack on the PG&E Metcalf substation in San Jose, CA – Mike Peters, OEIS

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, May 13, 2014 3:17 PM
To: [redacted]
Cc: Richard Sobonya; David Burnham
Subject: Re: Action Items from Today's Meeting
Attachments: 2014-04 Monthly Incident Report.pdf; DEPO Yearly Incident Report - 2013 (1).pdf

All,

Attached are examples of the monthly and yearly versions of the DEPO incident reports.

Thanks,

[redacted]

On Tue, May 13, 2014 at 1:31 PM, [redacted] wrote:
All,

As one of the follow-up actions from today's meeting, attached are the two memos. One is on the common OER event database proposal. Another is on the Performance Measure 3 approved by the Chairman in April.

Thanks!

[redacted]

On Tue, May 13, 2014 at 12:46 PM, [redacted] wrote:
All,

As discussed at our meeting this morning, attached is a presentation on the Div of Compliance Database, and below a list of the fields currently used, five of which are taken directly from the DEPO database.

Thanks!

[redacted]

Field	Source
Year	
Date-Event_Name	
ID	
Event_Date	DEPO
Event_Name	DEPO
Status	
NERC_Category	

[redacted]

DEPO Yearly Incident Report - 2013

[redacted]

Since incidents may be classified in multiple categories, the totals in the summaries may not be equal to the total number of incidents.

[redacted]

04/16/13 Metcalf 500 kV Substation Vandalism

Unknown suspects shot out the radiators for several 500/230 kV and 230/115 kV transformers and damaged breakers in the 115 kV yard at PG&E's Metcalf Substation. No load lost.

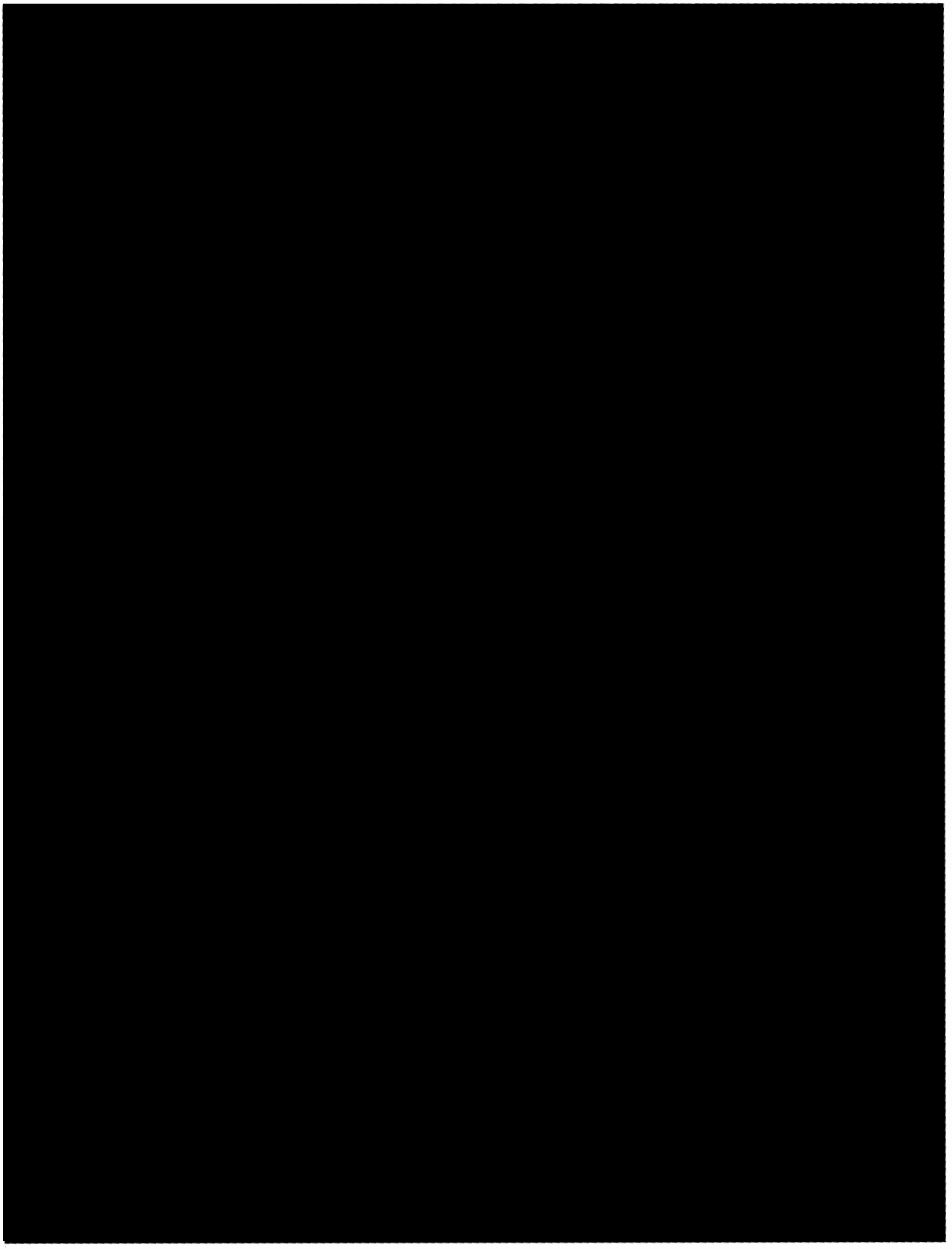
Causes: Unknown

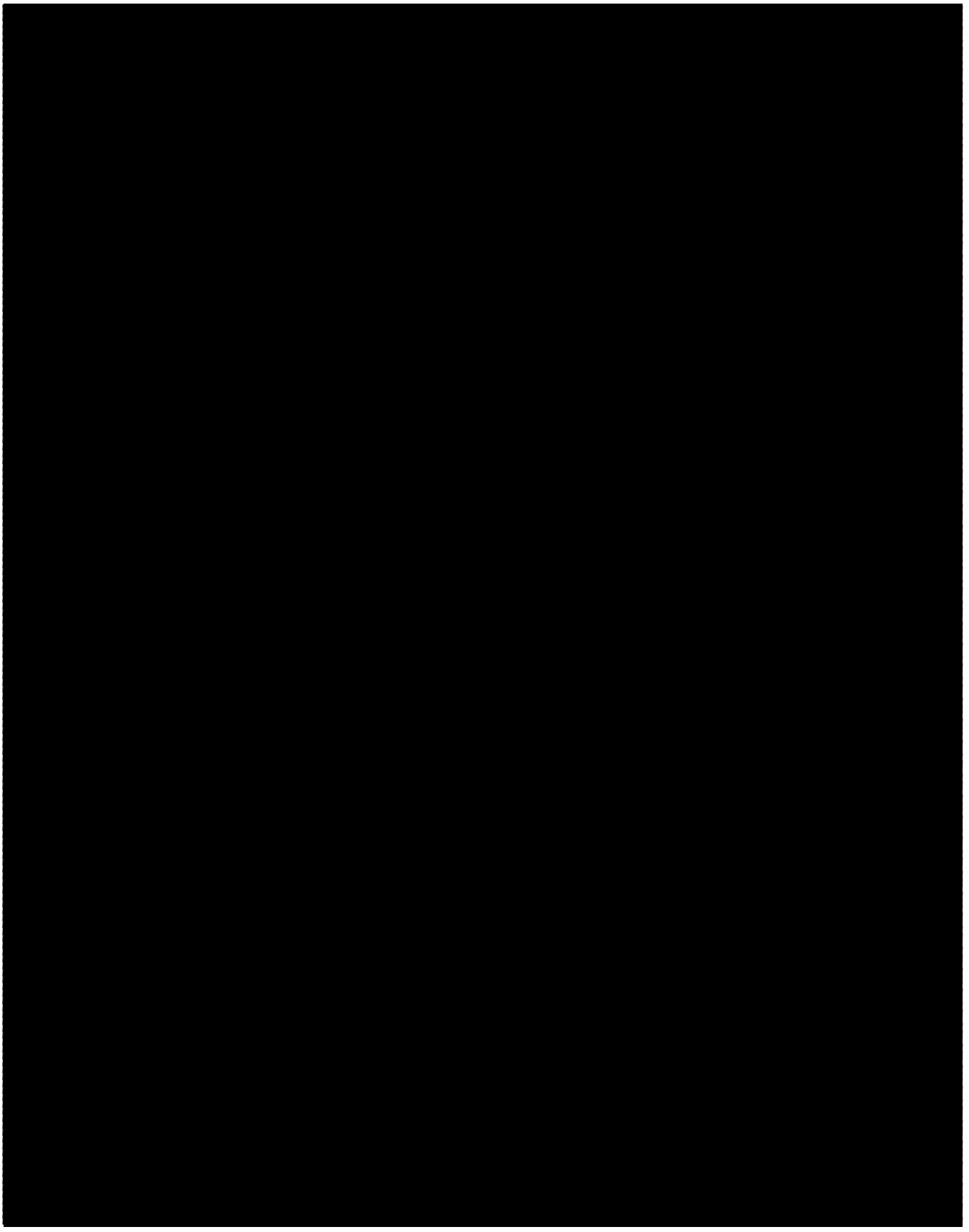
Results: Loss of substation equipment

Relevant Standards: TBD

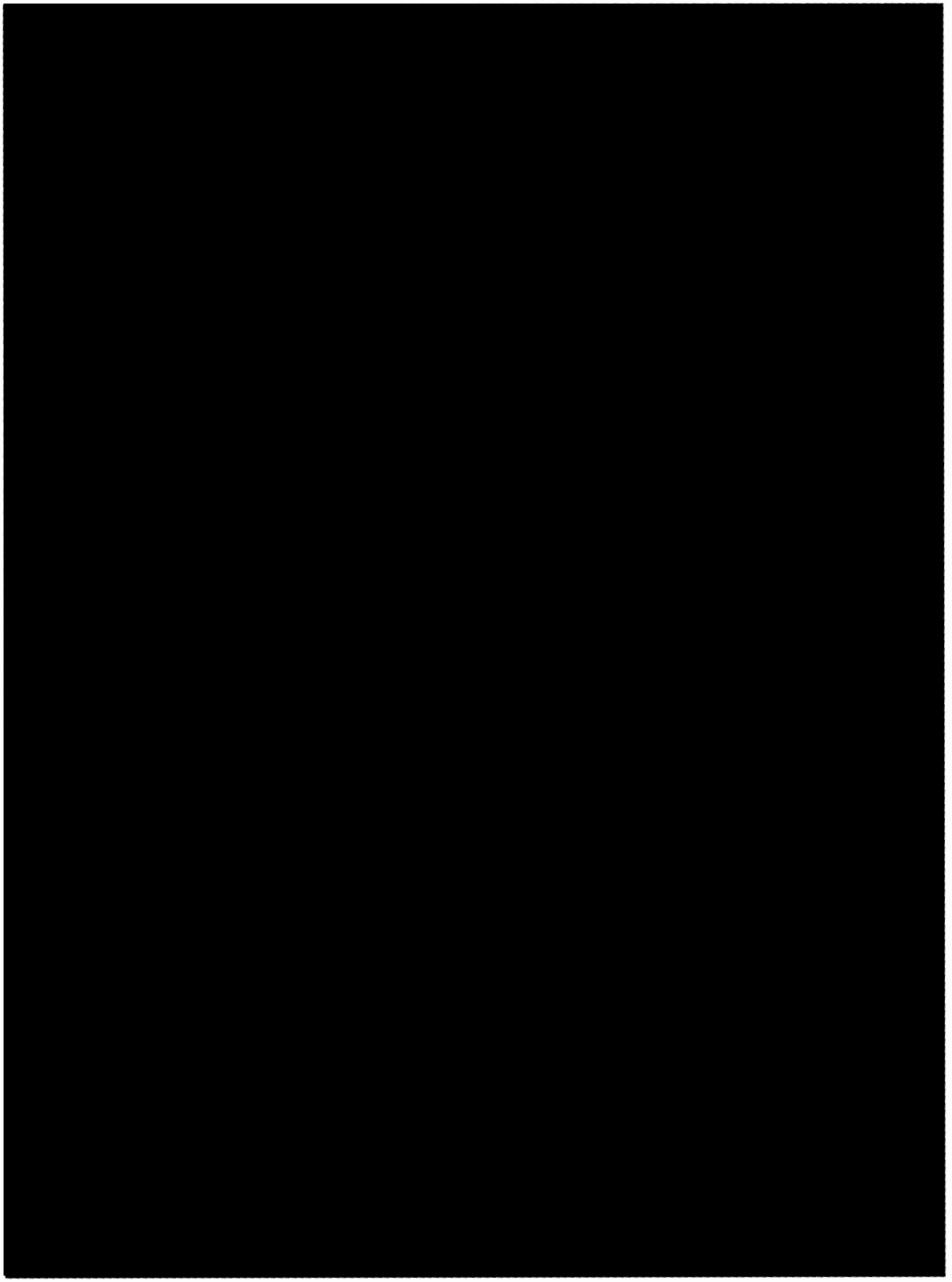
Reliability Coord: WECC

Regional Entity: WECC





Redacted Pursuant to FOIA Exemption B6_non-responsive



[redacted]

[redacted]

4/16/2013	Pacific Gas & Electric Co	Metcalf	Substation	500	Emergency Alert 1 Hour	Physical Attack	Vandalism	Repaired/Restored	At 0147 hr, suspect (s) unknown entered the 500 KV yard at Metcalf Substation (which is in San Jose, Calif) and shot out 2 or 3 transformer banks. The incident is currently under investigation, and law enforcement is present and looking for a secondary device.

[redacted]

[redacted]

From: Kal Ayoub
Sent: Tuesday, September 10, 2013 3:04 PM
To: [redacted]L
Cc: Michael Bardee; Edward Franks; Keith O'Neal; Cynthia Pointer
Subject: DRSS Bi-weekly Staff Meeting Agenda, 9/11/13, 2PM
Attachments: DRSS Bi-Weekly Staff Meeting Agenda 20130911.docx

DRSS - Please find attached the agenda for tomorrow's staff meeting at 2pm.

Thanks,
Kal

Kal Ayoub
Federal Energy Regulatory Commission
Manager, Division of Reliability Standards
Office of Electric Reliability
888 First Street, N.E. | Washington, D.C. 20426
Tel: 202.502.8863
Kal.Ayoub@ferc.gov

www.FERC.gov

[redacted]

DRSS Bi-Weekly Staff Meeting, 9/11/13, 2:00 PM – 3:30 PM

[redacted]

[redacted]

[redacted]

2. Presentation

- Physical attack on the PG&E Metcalf substation in San Jose, CA – Mike Peters, OEIS

[redacted]

Larry Parkinson [redacted]

From: [redacted]
Sent: Friday, February 07, 2014 10:44 AM
To: Norman Bay; Larry Gasteiger; ~~Roger Morie~~
Cc: Larry Parkinson; David Applebaum
Subject: Wellinghoff on NPR

In case any of you missed Wellinghoff's interview on NPR this morning re the sniper event at the PGE facility in San Jose, I attach.
There's a short written news story attached to the link for the radio broadcast, and a link to the WSJ article.
http://www.npr.org/blogs/thetwo-way/2014/02/06/272499102/sniper-attack-on-power-station-highlights-grids-vulnerability

[redacted]
Federal Energy Regulatory Commission
Office of Enforcement
Division of Investigations
[redacted]
Washington, DC 20426
[redacted]
(202)208-0057 (fax)

[redacted]

From: [redacted]
Sent: Thursday, March 06, 2014 10:08 AM
To: Edward Franks
Cc: [redacted] Keith O'Neal; Cynthia Pointer; [redacted]
Subject: RE: PHYSEC words as promised

Hey Ted, (et al, as promised),

Sorry to reply so late – my PC began acting up just as soon as I got out of town (digression omitted)... There wasn't much especially earthshaking on PHYSEC at CIPC this week, but there are a few noteworthy items:

- ES-ISAC staff has been leading a "PHYSEC outreach campaign," with PHYSEC SME from DOE, DHS, and ESCC in a supporting role. No names were dropped. Already completed in 8 cities; 5 more to come. [Matt Light, ES-ISAC staff).

- ES-ISAC intending to infuse recommended PHYSEC 'protocols' (practices, not necessarily 'best') into their web site under "Risk Information Sharing." [Matt Light]

- A PHYSEC advisory was issued last Friday, "quietly," in an attempt to keep it strictly within industry (for now anyway). No particulars were offered. [Matt Blizard, NERC staff]

- Bob Canada [NERC staff] noted that he released a "copper theft guide" on Monday (3/3/14). [Bob was former head of PHYSEC for Southern for many years.]

- Matt Blizard and Brian Harrell will be the leads for PHYSEC on NERC HQ staff. Both have considerable experience in PHYSEC, but little in Cyber.

- Jim Brenton (ERCOT, CIPC Vice-Chair) briefed events on the RISC front, saying that last week the trade assns. and NERC pitched that what they're doing now is adequate to need. Accordingly, "Metcalf got no traction with the RISC execs"... noting that RISC is not moving ahead with anything concerning PHYSEC at this time other then what's already afoot under CIPC (Guidelines). Brenton said he believes future emphasis will be on coordinated attacks, i.e., coordinated cyber, coordinated physical, coordinated hybrid. [Recall that RISC has been reconceived by Mr. Cauley and is now populated exclusively by industry execs; no longer tech SME as it had been in the past.]

- Bob Canada said NERC staff may get new tasking to undertake with GridEx sub-teams a "strategic assessment" to see where we stand adequacy-wise.

- Mark Engels (Dominion) briefed current progress/status on the 'three year and counting' "attack tree" analysis effort, and early fruit from the process points to a critical relationship between COMSEC and PHYSEC as key vulnerabilities with highest damage potential; with particular note on high leverage attainable from hybrid cyber/physical attacks. Also noted that "centralized attacks" pose the greatest attack surface (e.g., data centers)... [I believe I observed a collective groan from the multitude of the type "why did he say that out loud and in a public event?" [Mark knows his stuff and doesn't beat around the bush about his sentiments. My kinda' guy ☺]

- Report-out from PHYSEC WG (led by Canadian Ross Johnson) noted that a survey is currently in process concerning "PHYSEC training" (how much is being conducted at entities). [Sorry to report that I didn't catch whether it was NERC-wide or just Canada-wide, but suspect the latter.] For now, said they are "going with the recent PHYSEC Prep and Response guideline pubs; no new work on anything more currently on NERC's plate.

- INL is continuing to do work on baseline/background analysis concerning "armoring key assets." Note: There was a preliminary findings briefing conducted during last December's CIPC given by Ben Langhorst who is leading this research effort at INL (don't know if funding is from the DOE or DHS side of their house). That was in part the basis for my earlier thoughts forwarded to you as to industry concerns about how expensive hardening assets will be.

- Ross Johnson also noted that there is a bill moving through Parliament that has a staircase of penalties for sabotage of BES assets, including up to life imprisonment for conviction where loss of life is involved.

One further note: It was announced that the trade assns. (with NERC staff as tech back-up) will be conducting a "grid security briefing" for the House Homeland Security Committee on March 26th which will include treatment of PHYSEC as well as CyberSEC issues...

That's pretty much what happened PHYSEC-wise this week at CIPC...

[redacted]

[redacted]
Federal Energy Regulatory Commission (FERC),
Office Of Electric Reliability (OER),
Division of Reliability Standards
[redacted]

From: Edward Franks [mailto:edward.franks@ferc.gov]
Sent: Tuesday, March 04, 2014 10:24 AM
To: [redacted]
Subject: RE: PHYSEC words as promised

[redacted] Let me know how the conversation goes at the CIPC meeting on the topic of physical security.
Ted

[redacted]

From: [redacted]
Sent: Tuesday, December 03, 2013 8:16 AM
To: Harry Tom
Cc: [redacted]; [redacted]; [redacted]
Subject: Metcalf-experience PhySEC GL

Howdy,

I first learned of the existence of such a doc through a NERC-watching blogger (of good repute) who, without knowing it was NDA material, announced it to the world. "The world" in this case is several hundred industry folk with keen interest in CIP standards/GL development. Shortly thereafter, I received a few direct, casual inquiries about the subject GL, and just in the last week a couple more wondering if I'd be covering it at CIPC next week. [I understand Kathy Eads will be in attendance, but I don't think that's entirely relevant.] Bottom line, it's no secret, and also CIPC recently stood-up a new and active PhySEC subcommittee, with, last I heard, a roster of over 100 utility practitioners subscribed to the list serve. Barry explained that the blogger of note had it wrong in saying it "had been released to the industry," at least in so far as it's not general distribution; but rather select and subject to NDA. So I get all that... Barry also requested that I write to you in further inquiry about this, copying those listed.

I feel the need to review a copy of what we're telling even a few Responsible Entities about the matter – NDA notwithstanding, they talk, trust me. And 'while they're at it' grilling me on CIP V5 next week, I have every expectation I'll get more limited but similar impatiently intoned query on this GL as well. I don't need it because I need to explain it – it's NDA – but I would like to be able to dance around the edges with some accuracy. I haven't seen it – how does it stack up against American Society for Industrial Security GL's – they are pretty much 'the bible' outside MIL/INTEL circles? What do I have to do to get a copy? I'll be happy to sign an NDA. Someone over here in standards-land needs to be apprised... Thanx...

Best Regards,

[redacted]

[redacted]

Critical Infrastructure Protection Advisor
Federal Energy Regulatory Commission (FERC),
Office Of Electric Reliability (OER),
Division of Reliability Standards

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, December 03, 2013 7:24 AM
To: [redacted]
Subject: PhySEC GL

Did we ever receive copy on the post-Metcalf mystery GL Joe and friends distributed sans our notification? If not, how do you suggest we raise hell? This is BS, and I'm just the guy to escalate absent another approach. I will be pilloried on it at CIPC next week and I need to review it in advance.

Thanx

[redacted]
Critical Infrastructure Protection Advisor
Federal Energy Regulatory Commission (FERC),
Office Of Electric Reliability (OER),
Division of Reliability Standards
[redacted]

[redacted]

From: [redacted]
Sent: Thursday, November 14, 2013 3:52 PM
To: [redacted]
Subject: FERC 'Confidential' Physical Security Guideline

[redacted]

As much a heads-up as anything...

Today on a national webex Tom Alrich of Honeywell reported that FERC had released the subject document "to industry" in response to the PG&E Metcalf substation incident. Any idea if/when it might be confidentially released to staff, CIP SME at least?

Thanx,

[redacted]

[redacted]
Critical Infrastructure Protection Advisor
Federal Energy Regulatory Commission (FERC),
Office Of Electric Reliability (OER),
Division of Reliability Standards
[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, July 09, 2013 2:56 PM
To: [redacted]Keith O'Neal; Cynthia Pointer; Edward Franks
Subject: NERC CIPC Notes/slides - June ATL

Greetings,

Materials from the most recent NERC CIPC meeting can be found in the folder below. Included is the agenda, NERC's draft minutes, a zipped presentations file, and [redacted] notes (with certain items of interest highlighted). Many of the slide decks are pretty wordy and the talks move right along, so please excuse the instances of "please see slides" in my notes.

Especially noteworthy was the presentation by PG&E about the armed attack (many bullets) on their Metcalf substation in Silicon Valley. His slides should be in the presentation deck (so I'm told – haven't looked myself), and I took notes in as much detail as I could (within my 'notes' doc.).

P:\OER[redacted]Cyber Archives\NERC CIPC\2013 CIPC Summer Mtg – Atlanta

Best regards,

[redacted]
Critical Infrastructure Protection Advisor
Federal Energy Regulatory Commission (FERC),
Office Of Electric Reliability (OER),
Division of Reliability Standards
[redacted]

NERC CIPC June 12 & 13 2013

NOTE: See NERC Minutes posted after the meeting

Matt Blizard – Dir CIP, NERC

- Most outstanding Task Force reports due to be presented at August BOT
- ESCC to be taken over/run by industry CEOs

PG&E briefing on 4/16/2013 physical security event (gun shots) at Metcalf substation

Tom Burgess – NERC Staff - BES Re-definition Project

- Order 773 773A approved re-definition
- Asked FERC for in-service relief of extra year to attend new regulatory/legal liability exposure (TBD)
- Major feature of new paradigm is bright line of 100kv (in/out); removes Regional flex in determination
- Had no answer ("good question") as to why cyber assets were excluded from consideration

Laura Brown (NERC Staff) – EO & PPD [Just there of the WGs; NERC closely participating in these]

- Cyber Dependent Infrastructure (something) WG
- Framework Collaboration WG (Donna Dobson) – Draft framework due by next mtg (San Diego)
- Evaluation and Planning WG – re-doing the NIPP; assembling writing teams – Oct due to Pres

Melanie Seader – EEI – Washington Watch Report

- House Intel Sharing and Protection Act – passed House; not brought to floor of Senate yet
- Securing America's Future: The Cybersecurity Act of 2012 – Senate; more regulatory in nature
- EEI thinks Senate will remain quiescent awaiting to see shake-out of EO action
- Grid Act – from last year; would expand FERC regulatory authority; died in last session Congress
- Markey-Waxman – says shortcomings in response to NERC GLs would be fixed by FERC via Grid Act

Jim Brenton – RISC report-out – slides explain process – Next mtg in DC on July 12th

- Risk Gap Analysis effort coming: review ERO activities; rate hi/med/low risks; annual effort
- See slides for digression
- Subcommittee Status Reports

Operating Security SC – Carl Eng – see slide 15 on recommended consolidation for info sharing processes

Bill Lawrence – NERC – GridEx II – https://events.signup4.com/gridex2 Are we participating?

Cyber Attack Task Force – Mark Engels:

- Only six RE reps involved, but this is seen as an advantage (Mona Lisa not painted by committee)
- Completed AT training in April
- Looking at it strictly on the operations frame of reference, specifically the BA function
- Systems-specifics cause/effect to be taken up as a second pass
- "Constantly recurring random events" – pervasive, hard to factor into threat/event trending
  - Gear going up/down due to outage
  - Gear going up/down for maintenance
  - Other random events affecting BES (GMD, Superbowl, weather)
- Seek to identify situational awareness instances of ops action unintentionally eroding tolerances

Personnel Clearance TF – Nathan Mitchell - Report approved at mtg:

- has a 'clearance process model' for nominating candidates
- Pushing for SCI clearances for some;
- propose multiple sponsoring agencies;
- revocation barely even noted;
- say the government (notably DHS) will pay for EBIs... (Good luck!)

Security Metrics Framework TF - Jamie Sample – work/direction (to date) approved at meeting

- At this point trying to define what "leading and trailing" indicators are to be (report elements)
- Buzzword is "Experience Sharing Tool"
- Tool will have a page on ES-ISAC site for entity to report sought data element examples
- Will "generate first quarterly report on security metrics 'at' Fall CIPC meeting"
  [NORT: This hasn't been worked until last 3-4 months; product within 90days? Improbable...]
- Brenton noted event info collection required by CIPs is not being aggregated across industry
- Anonymously submitted data will be held as such and preserved in aggregation
- Now drawing-off info collected at ICS-CERT and populating tool

Compliance and Enforcement WG – Paul Crist – have barely gotten started [Tobias now involved]

- Interesting area to be pursued is consequences for virtual systems/networks

Cybersecurity Events Analysis WG – Eric Warakomski – still populating team roles (seems redundant)
CSSWG – reported at last meeting completed its active work; looking for new project ideas

ES-ISAC Update – Ben Miller (NERC) com

- Argued need for sector-specific data distinct from others...
- Proposed rule of thumb: If takes > 15 min to write exec sum for mngt, should report to ISAC
- Brenton said that ES-ISAC aegis is ALL sector incidents, i.e., ICS IT, market, distribution, etc.

Physical Security WG - Ross Johnson – plea for volunteers; no serious progress; charter approved

Physical Security Response Guideline TF – John Breckenridge – Overview in slides

- Reduced number of threat levels from 5 to 3
- !! Contains flipchart-type Appx meant to be printed and shared with field mngt/teams that can be used in real time on short notice; expl: "Elevated, Items 12, 15, 21... Looks excellent

Security Training WG – William Whitney – still ramping-up

- Won't be providing training per se; will work to arrange pre-CIPC-meeting courses
- Have combined phy- and cyber- security training
- Assembling a list of free on-line training sites from all sources
- Soliciting subjects for workshops, mini-courses, briefings...

Procurement Language Update for Energy Sector Control Systems – Ed Goff

- This is an ESCSWG initiative (of which NORT is a member)
- Working on 3rd Rev of procurement language doc (1st NY/SANS; then 2nd 'DHS's from INL)
- Looking to synthesize commonalities between different similar instruments from elsewhere
- Wordy slides – read as interested; update to be finalized by end of January 2014

GridSecCon 2013 Conference (Oct 15-17 Jacksonville) – Bill Lawrence – mostly advertising – see Slides

Cybersecurity Standards Update –Scott Mix – Standing in for Noess

- Talked about V5 NOPR; possibilities re how will V5 affect V4 effective date

Sufficiency Review Overview (Outreach) – Scott Mix – Really wordy slides that explain it all... Parts:

- RBAM V3 sufficiency – how did it work out; lessons learned, etc.;
- Ver. 3-4-5 transition planning discussed in review, as well as stuff like Aurora
- If there's discovery of a major exposure to BPS, it will be referred to compliance authorities
- Discussed with SR participants Para 81, and new "RAI" internal controls approach
- Many recommendations to participants include practices that go beyond strict CIP requirements
- See the report on the (new) NERC web site – link at end of Scott's presentation

Compliance – Tobias Whitney

- Until V5 Order published, have to assume V4 goes into effect 4/1/14
- Adherence to V3 will still be required until V5 effective date – 'interesting' transition issues
- Tobias says they will be flexible and accommodating as much as possible in interim
- ... Lots of questions/discussion on hypotheticals

[redacted]

From: [redacted]
Sent: Wednesday, April 16, 2014 3:24 PM
To: [redacted]
Subject: FW: Blast Protection Paper
Attachments: Presentation 6_Dr Braden Lusk NERC 3-7-12_final.pptx

This is what I sent.

Thanks for your help!
[redacted]

From: [redacted]
Sent: Wednesday, April 16, 2014 3:20 PM
To: [redacted]
Cc: [redacted] Edward Franks
Subject: FW: Blast Protection Paper

All,

I asked [redacted] about the University of Kentucky ballistics study that SERC mentioned in our meeting earlier. [redacted] found the attached presentation from Dr. Braden Lusk from the March 2012 CIPC meeting. He also mentioned that he remembered a previous study performed on a similar topic in 2001-2003 by Larry Dolci of KCP&L that was presented to the CIPAG (CIP advisory group).

While the work that he did looks fun, I'm not sure how useful his recommendations or findings are. His main two recommendations from slide 5 are:

- Transformer components are naturally resilient to blast induced damage from assessed threats.
- Providing adequate distance between the target and threat (standoff) is enough to ensure protection from blast damage.

His first recommendation is invalid considering that the Metcalf attack showed that weaponry can be used to bring down transformers (he does not appear to have considered the threat of as many rounds of weaponry as were used in the Metcalf attack). The second result appears invalid now too as standoff distance may be a mitigating factor, but is not expected to "ensure protection from blast damage." This presentation does not appear to be the final report from his work (which neither I nor [redacted] could find a copy of). [redacted] good friends with Bob Canada though, so if someone does want to see the final report, we can ask.

As an additional note, Dr. Braden Lusk is a mining engineer that appears to specialize in blasts in coal mining operations, so I am uncertain how they selected him for the ballistic study performed for the CIPC. Let me know if you have any other questions.

Thanks,
[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, February 05, 2014 5:23 PM
To: [redacted] Edward Franks
Subject: FW: WSJ & Metcalfe Attack

FWIW... Ross is an earnest and seemingly capable guy (also a Canadian) who has actively assumed the Chair of the CIPC PHYSEC WG...

[redacted]

From: Ross Johnson [mailto:rjohnson@capitalpower.com]
Sent: Wednesday, February 05, 2014 2:26 PM
To: psrg
Subject: WSJ & Metcalfe Attack

All,

This link is to an interesting article in the Wall Street Journal on last year's attack at the Metcalf Substation.

http://online.wsj.com/news/article_email/SB10001424052702304851104579359141941621778-lMyQjAxMTA0MDAwNDEwNDQyWj

Best regards,
Ross

Ross Johnson, CPP
Senior Manager, Security & Contingency Planning
Capital Power Corporation
10th Floor, EPCOR Tower
1200-10423 101 Street NW
Edmonton, Alberta
Canada T5H 0E9

Office +1 (780) 392-5482
[redacted]

Y

[redacted]

From: [redacted]
Sent: Wednesday, February 05, 2014 5:48 PM
To: [redacted] Sanders, William H'; janorton@[redacted]
Subject: WSJ & Metcalfe Attack

Howdy,

This link is to a very interesting article in the Wall Street Journal on last year's attack at the Metcalf Substation in San Jose.

http://online.wsj.com/news/article_email/SB10001424052702304851104579359141941621778-lMyQjAxMTA0MDAwNDEwNDQyWj

[redacted]

[redacted] [redacted]

From: [redacted]
Sent: Friday, February 07, 2014 9:27 AM
To: [redacted]
Cc: Cynthia Pointer; Keith O'Neal; Edward Franks
Subject: NPR had Wellinghoff & Metcalf this morning

http://www.npr.org/blogs/thetwo-way/2014/02/06/272499102/sniper-attack-on-power-station-highlights-grids-vulnerability

Cordially,

[redacted]
Office of Electric Reliability (OER)
Federal Energy Regulatory Commission
[redacted]

[redacted] [redacted]

From: [redacted]
Sent: Monday, April 14, 2014 8:31 AM
To: [redacted]ferc.gov; [redacted]@ferc.gov
Subject: Energy Policy article- if you subscribe

http://www.electricitypolicy.com/index.php?option=com_content&view=article&id=6726

Pacific Gas and Electric is offering a $250,000 reward for information leading to the arrest and conviction of those who fired gunshots that severely damaged PG&E's Metcalf substation near San Jose a year ago. In a press release, the San Francisco utility said **it will invest about $100 million** over the next three years on substation security at its highest priority facilities, including "enhanced intruder detection systems and buffer zones through additional fencing."

[redacted]
Federal Energy Regulatory Commission
Office of Electric Reliability (OER)
Division of Standards and Security, SG-1
[redacted]

[redacted]

From: Michael Bardee
Sent: Tuesday, April 16, 2013 1:45 PM
To: Joseph McClelland; ~~Harry Tom~~
Subject: Fwd: Flex-Alert issued for Northern California only
Attachments: 20130416_ISO FlexAlertPressRelease_Urgent_conservation_needed_NOW_in_Santa_Clara_and_Silicon_Valley.pdf

---------- Forwarded message ----------
From: **Ulmer, Andrew** <aulmer@caiso.com>
Date: Tue, Apr 16, 2013 at 1:40 PM
Subject: RE: Flex-Alert issued for Northern California only
To: "Michael.Bardee@ferc.gov" <Michael.Bardee@ferc.gov>

Mike:

I wanted to alert you to this matter at the Metcalf substation. The California ISO has requested conservation through the issuance of a Flex-Alert.

Andrew

Andrew Ulmer

Director, Federal Regulatory Affairs

California ISO

Work (202) 239-3947

[redacted]

FLEXALERT.ORG **FLEX ALERT**

California ISO
Shaping a Renewed Future

April 16, 2013

Contact: ISO Media Hotline (888) 516-NEWS

Stephanie McCorkle: 916 802-4033
Steven Greenlee: 916 990-4295

CONSERVATION TIPS

- Lower lighting.
- Turn off thermostats.
- Power down unnecessary electric appliances and devices.

STAGE 1 EMERGENCY
Operating reserves forecast to fall to between 7% - 6%

STAGE 2 EMERGENCY
Operating reserves forecast to fall below 5%

STAGE 3 EMERGENCY
Operating reserves forecast to fall below 3%

TRANSMISSION EMERGENCIES

Declared when local voltage levels are at risk due to sudden power line outages or when fires threaten the grid.

Flex-Alert for Northern CA Only Urgent conservation needed NOW in Santa Clara & Silicon Valley

The California ISO is urging residents and businesses in the San Jose area, in particular Santa Clara and Silicon Valley, to conserve electricity NOW following heavy damage to the Metcalf transmission substation.

Pacific Gas and Electric is reporting heavy damage to transformers at the substation following gunshots heard during an apparent vandalism in the early morning hours. Santa Clara law enforcement is working closely with PG&E to investigate.

As damage assessments continue, additional equipment at the substation may be taken out-of-service. This will limit transmission capability in this area of the high-voltage grid, which is why conservation is required.

Consumers are urged to reduce their energy use now through midnight. The ISO will keep media informed. For more information go to www.caiso.com

Monitor grid conditions at www.caiso.com. Click "Notify me" to sign up for *Flex Alerts* and other updates.

[redacted] [redacted]

From: Michael Bardee
Sent: Tuesday, April 16, 2013 1:44 PM
To: David Andrejcak; ~~Nano Sierra~~
Subject: Fwd: Flex-Alert issued for Northern California only
Attachments: 20130416_ISO FlexAlertPressRelease_Urgent_conservation_needed_NOW_in_Santa_Clara_and_Silicon_Valley.pdf

This may be old news but just in case....

---------- Forwarded message ----------
From: **Ulmer, Andrew** <aulmer@caiso.com>
Date: Tue, Apr 16, 2013 at 1:40 PM
Subject: RE: Flex-Alert issued for Northern California only
To: "Michael.Bardee@ferc.gov" <Michael.Bardee@ferc.gov>

Mike:

I wanted to alert you to this matter at the Metcalf substation. The California ISO has requested conservation through the issuance of a Flex-Alert.

Andrew

Andrew Ulmer

Director, Federal Regulatory Affairs

California ISO

Work (202) 239-3947

[redacted]

FLEX ALERT
FLEXALERT.ORG

California ISO
Shaping a Renewed Future

April 16, 2013

Contact: ISO Media Hotline (888) 516-NEWS

Stephanie McCorkle: 916 802-4033
Steven Greenlee: 916 990-4295

CONSERVATION TIPS

- Lower lighting.
- Turn off thermostats.
- Power down unnecessary electric appliances and devices.

STAGE 1 EMERGENCY
Operating reserves forecast to fall to between 7% - 6%

STAGE 2 EMERGENCY
Operating reserves forecast to fall below 5%

STAGE 3 EMERGENCY
Operating reserves forecast to fall below 3%

TRANSMISSION EMERGENCIES

Declared when local voltage levels are at risk due to sudden power line outages or when fires threaten the grid.

Flex-Alert for Northern CA Only Urgent conservation needed NOW in Santa Clara & Silicon Valley

The California ISO is urging residents and businesses in the San Jose area, in particular Santa Clara and Silicon Valley, to conserve electricity NOW following heavy damage to the Metcalf transmission substation.

Pacific Gas and Electric is reporting heavy damage to transformers at the substation following gunshots heard during an apparent vandalism in the early morning hours. Santa Clara law enforcement is working closely with PG&E to investigate.

As damage assessments continue, additional equipment at the substation may be taken out-of-service. This will limit transmission capability in this area of the high-voltage grid, which is why conservation is required.

Consumers are urged to reduce their energy use now through midnight. The ISO will keep media informed. For more information go to www.caiso.com

Monitor grid conditions at www.caiso.com. Click "Notify me" to sign up for *Flex Alerts* and other updates.

[redacted]

From: Michael Bardee
Sent: Tuesday, April 16, 2013 4:09 PM
To: David Andrejcak; Nano Sierra; ~~Eddy Lim~~
Cc: Edward Franks
Subject: Fwd: FW: CAISO Conservation Alert

We should assist OEIS in any way we can. [redacted] I told him you were in CA and could go to Folsom if helpful.

---------- Forwarded message ----------
From: **Joseph McClelland** <joseph.mcclelland@ferc.gov>
Date: Tue, Apr 16, 2013 at 4:00 PM
Subject: FW: CAISO Conservation Alert
To: Michael Bardee <michael.bardee@ferc.gov>

From: Jon Wellinghoff [mailto:jon.wellinghoff@ferc.gov]
Sent: Tuesday, April 16, 2013 3:40 PM
To: Joseph McClelland
Subject: Fwd: CAISO Conservation Alert

Please get me all the details as soon as you can.

Thanks,

Jon

Jon Wellinghoff

FERC

888 1st Street NE

Washington, DC 20426

Office 202.5026580

---------- Forwarded message ----------
From: **Emergency BB2** <emergency.bb2@ferc.gov>
Date: Tue, Apr 16, 2013 at 1:59 PM
Subject: CAISO Conservation Alert
To: Jon.Wellinghoff@ferc.gov, Philip.Moeller@ferc.gov, John.Norris@ferc.gov, Cheryl.LaFleur@ferc.gov, tony.clark@ferc.gov, James.Pederson@ferc.gov, norman.bay@ferc.gov, Larry.Gasteiger@ferc.gov, David.Morenoff@ferc.gov, Martin.Kirkwood@ferc.gov, Michael.McLaughlin@ferc.gov, Anna.Cochrane@ferc.gov, Jeff.Wright@ferc.gov, Ann.Miles@ferc.gov, Jamie.Simler@ferc.gov,

Mason.Emnett@ferc.gov, Joseph.McClelland@ferc.gov, Leonard.Tao@ferc.gov, Chris.Murray@ferc.gov, anton.porter@ferc.gov
Cc: Michael.Bardee@ferc.gov, Edward.Franks@ferc.gov, David.Andrejcak@ferc.gov, Nano.Sierra@ferc.gov, Jonathan.First@ferc.gov, commissionersassistants@ferc.gov

From the Office of Electric Reliability:

The California ISO has issued a Flex Alert for customers in Northern California (Santa Clara and Silicon Valley areas), to immediately begin electricity conservation measures due to damage at the Metcalf substation, which occurred early this morning. CAISO reports the grid is in stable condition and this incident is only impacting a small load pocket in the general area near Metcalf Substation.

Pacific Gas and Electric earlier reported gunshot damage to transformers at the substation, around 2:00 AM Pacific Time today. Santa Clara law enforcement is working closely with PG&E in this investigation.

As damage assessments continue, additional equipment at the substation may be taken out-of-service, and may limit transmission capacity in this area. No further details are available at this time with regard to the extent or expected return to service of the equipment that has been damaged.

We will continue to monitor the situation and provide details as they become available.

[redacted]

From: Michael Bardee
Sent: Wednesday, April 17, 2013 7:26 AM
Cc: Edward Franks; David Andrejcak; Nano Sierra; Richard Sobonya
Subject: Re: FW: Metcalf Substation

[redacted]

On Wed, Apr 17, 2013 at 7:04 AM, Joseph McClelland <joseph.mcclelland@ferc.gov> wrote:

From: [redacted]
Sent: Tuesday, April 16, 2013 5:50 PM
To: [redacted] Joseph McClelland
Subject: Metcalf Substation

Attached is a draft of the report for the Chairman. Please review and comment to the group. I will maintain the document. Thank you.

[redacted]

Federal Energy Regulatory Commission
Office of Energy Infrastructure Security (OEIS)
888 First Street NE, 91-57
Washington, DC 20426

[redacted]

[redacted] [redacted]

From: Michael Bardee
Sent: Wednesday, April 17, 2013 8:00 AM
To: Joseph McClelland
Cc: Edward Franks; David Andrejcak; Nano Sierra; Richard Sobonya
Subject: Re: FW: Metcalf Substation

Joe: [redacted]

- Mike

On Wed, Apr 17, 2013 at 7:04 AM, Joseph McClelland <joseph.mcclelland@ferc.gov> wrote:

From: [redacted]
Sent: Tuesday, April 16, 2013 5:50 PM
To: [redacted] Joseph McClelland
Subject: Metcalf Substation

Attached is a draft of the report for the Chairman. Please review and comment to the group. I will maintain the document. Thank you.

[redacted]

Federal Energy Regulatory Commission
Office of Energy Infrastructure Security (OEIS)
888 First Street NE, 91-57
Washington, DC 20426

[redacted]

[redacted] [redacted]

From: Michael Bardee
Sent: Wednesday, February 05, 2014 6:23 PM
To: Joseph McClelland
Cc: Joshua Konecni; Leonard Tao; Chris Murray; Edward Franks; David Morenoff; Martin Kirkwood; Christy Walsh; [redacted]
Subject: Re: Industry Response to WSJ Physical Security Story

[redacted]

Sent from my iPad

On Feb 5, 2014, at 4:08 PM, Joseph McClelland <joseph.mcclelland@ferc.gov> wrote:

[redacted]

Sent from my iPad

Begin forwarded message:

From: "Aaronson, Scott" <SAaronson@eei.org>
To: "Hoffman, Patricia" <Pat.Hoffman@hq.doe.gov>, "adam.cohn@hq.doe.gov" <adam.cohn@hq.doe.gov>, "ahsha.tribble@hq.doe.gov" <ahsha.tribble@hq.doe.gov>, "caitlin.durkovich@hq.dhs.gov" <caitlin.durkovich@hq.dhs.gov>, "Schreiber, Tonya (tonya.schreiber@hq.dhs.gov)" <tonya.schreiber@hq.dhs.gov>, "Alt, Richard (richard.alt@HQ.DHS.GOV)" <richard.alt@hq.dhs.gov>, "'Enrique.Matheu@HQ.DHS.GOV' (Enrique.Matheu@HQ.DHS.GOV)" <Enrique.Matheu@hq.dhs.gov>, Summer Snyder <summer.snyder@hq.dhs.gov>, "McGlone, James (James.McGlone@hq.doe.gov)" <James.McGlone@hq.doe.gov>, Rhonda Dunfee <rhonda.dunfee@hq.doe.gov>, "michael.smith2@hq.doe.gov" <michael.smith2@hq.doe.gov>, "joseph.mcclelland@ferc.gov" <joseph.mcclelland@ferc.gov>, "Cathy Eade (cathy.eade@ferc.gov)" <cathy.eade@ferc.gov>
Subject: Industry Response to WSJ Physical Security Story

I wanted to share this email with our government partners so that you could see how the industry is talking about today's front page WSJ article. Please note the many references to the government-industry partnership, and our appreciation for the substantial progress that's been made as a result of this relationship.
Below is the message that Tom Kuhn sent to our member company CEOs and their DC offices this afternoon along with attached talking points. We have dealt with additional media inquiries throughout the day and have made many references to the substation outreach campaign, the ESCC, GridEx II, and other examples of the shared responsibility government and industry have taken in the name of critical infrastructure protection.
Please feel free to share with your public affairs offices, and don't hesitate to contact me if you

have any questions. Many thanks, as always, for all you do.

Scott I. Aaronson
Edison Electric Institute, Government Relations
O: (202) 508-5481 | M: (202) 569-8804

From: Kuhn, Thomas [mailto:TKuhn@eei.org]
Sent: Wednesday, February 05, 2014 2:36 PM
To: EEI Member Company CEOs and Washington Reps
Subject: Wall Street Journal Story on Physical Security
Importance: High

A front-page story<http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778?mod=WSJ_hp_RightTopStories> in today's Wall Street Journal chronicles last year's attack on the Metcalf facility and characterizes the grid as vulnerable to physical attacks. As you know, our industry is well aware of the incident and is working in partnership with senior Administration officials from all relevant agencies to address physical security issues. We also are keeping Congress informed of our efforts to deal with both cyber and physical security threats.

This story is already generating significant interest. We have developed the attached talking points to respond to media and stakeholder inquiries.

Chad Sweet, former CIA and DHS official and co-founder and CEO of the Chertoff Group, appeared this morning on Fox News<http://www.foxnews.com/on-air/happening-now/index.html#/v/3156531062001>. Sweet reaffirmed that our industry is very focused on resiliency and highlighted that we are working in partnership with the government to address security issues. The Chertoff Group advises EEI on national security issues.

As always, please feel free to contact me if you have any questions, or ask your staff to contact Scott Aaronson at 202-508-5481 or saaronson@eei.org<mailto:saaronson@eei.org> (technical/national security) or Stephanie Voyda at 202-508-5612 or svoyda@eei.org<mailto:svoyda@eei.org> (communications).

cc: Washington Reps

[redacted] [redacted]

From: Michael Bardee
Sent: Friday, February 21, 2014 3:41 PM
To: Edward Franks; Martin Kirkwood; [redacted]
Subject: Fwd: I/C (Sen. Schumer) bulk power system, security (2014-00008)
Attachments: 2014-00008.pdf; control sheet.pdf

fyi

---------- Forwarded message ----------
From: [redacted]
Date: Fri, Feb 21, 2014 at 3:29 PM
Subject: I/C (Sen. Schumer) bulk power system, security (2014-00008)
To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring <Andrea.Spring@ferc.gov>, Andrew Weinstein <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>, David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>, Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>, John Peschke <john.peschke@ferc.gov>, Joshua Konecni <Joshua.Konecni@ferc.gov>, Kim Shannon <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura Vendetta <laura.vendetta@ferc.gov>, Leonard Tao <leonard.tao@ferc.gov>, Mark Hershfield <mark.hershfield@ferc.gov>, Mary O'Driscoll <Mary.O'Driscoll@ferc.gov>, Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee <Michael.Bardee@ferc.gov>, Nicholas Tackett <nicholas.tackett@ferc.gov>, Patricia Herrion <Patricia.Herrion@ferc.gov>, Robert Ivanauskas <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks <russell.fairbanks@ferc.gov>, Sandra Waldstein <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>, Shawn Bennett <Shawn.Bennett@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
Cc: "[redacted] Craig Cano <craig.cano@ferc.gov>, Joseph McClelland <joseph.mcclelland@ferc.gov>

FOR YOUR INFORMATION ONLY.

DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR BEFORE 02/28/14.

--
[redacted]
Office of External Affairs
[redacted]

CHARLES E. SCHUMER
NEW YORK

United States Senate

WASHINGTON, DC 20510

COMMITTEES:
BANKING
DEMOCRATIC POLICY & COMMUNICATIONS
FINANCE
JUDICIARY
RULES

February 17, 2014

The Honorable Jeh Johnson
Secretary
U.S. Department of Homeland Security
301 7th Street Southwest
District of Columbia, 20024

The Honorable Cheryl LaFleur
Acting Chairman
Federal Energy Regulatory Commission
888 1st Street NE
Washington, D.C. 20426

Dear Secretary Johnson and Chairman Lafleur:

I write to urge that your agencies act quickly to develop and enforce more stringent standards regarding physical security at substations and other critical facilities necessary to ensure the reliability of the bulk electric power system. A successful attack last April on Pacific Gas & Electric's Metcalf transmission substation – which severed transmission cables and nearly and nearly shut down the substation, almost caused a large-scale blackout in California and surrounding states and shows the need to improve physical security standards to protect critical electric infrastructure from future attacks. According to Section 1211 of the Energy Policy Act of 2005 (EPAct 2005), FERC has the ability to utilize its authority to determine whether new minimum standards regarding physical security are needed to ensure the reliability of the power grid. Virtually every aspect of our nation's way of life, from powering our homes and businesses, to transportation and manufacturing, relies on the reliable generation and delivery of electric power. We must actually quickly to prevent another attack form successfully causing widespread damage to our electric infrastructure and the concomitant reliability challenges associated with such an event.

As you are aware, on April 16, 2013, a group of snipers destroyed 17 transformers at an electrical substation in San Jose, California. This attack, which lasted almost 20 minutes, nearly brought down power to all of Silicon Valley. The perpetrators have not yet been caught. This attack underscores how vulnerable our entire electrical grid is to domestic and foreign terrorism, and the need for enhanced safety measures. Furthermore, recent reports have revealed that the attack on the Metcalf substation in California was not the first time that critical electric infrastructure in the U.S. has been targeted by terrorists. According an article in *The Wall Street Journal*, there were 274 major instances of vandalism or deliberate damage to U.S. power plants in the past three years. The article also mentions that terrorist attacks on power plants are a major problem overseas, with 3,000 attacks having been carried out on power lines, towers or substations between 1996 and 2006. Though some steps have been made to protect the grid from physical attacks, more must be done to enact minimum standards. I commend some of the steps some leading companies in the electric power industry and federal agencies have taken to reduce the risk of a physical attack, but voluntary measures by some companies are no substitute for assurances that the power of enforceable standards have for ensuring that all electric power entities that play significant role in the reliability of our electric power infrastructure are taking the appropriate steps and putting in place necessary measures. Given the interdependent and cascading nature of the electric power grid and the reliability challenges it faces, which flows

2014-00008

across different states and utilities, we must make sure that all of the key players are implementing equally strong standards.

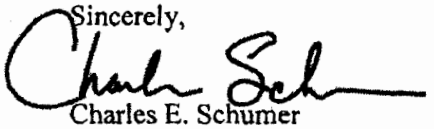
According to Section 1211 of the Energy Policy Act of 2005 (EPAact 2005), both the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) have the authority to determine whether additional minimum standards regarding physical security at critical substations and other facilities critical to the reliability of the bulk power system. NERC, which is comprised of industry representatives develops and proposes physical security standards while the FERC gives them final approval. While I appreciate that current law calls for mandatory standards to be developed in close consultation with industry, I feel that FERC and DHS must act quickly in order to respond to rapidly emerging threats. Under the current approach, consensus is required between both FERC and NERC to mandate protections, and proposed standards that do not receive support from both NERC and FERC can become voluntary. The process of reaching consensus can often take years, lagging far behind the pace at which new threats develop.

The reasons for moving forward with stronger physical security standards are clear and unmistakable. The Department of Homeland Security's Presidential Policy Directive (PPD) 21, which was issued last March to address critical infrastructure security and resilience identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation. The reliance of virtually all industries on electric power and fuels means that all sectors have some dependence on the Energy Sector. All entities at the table, FERC, NERC, DHS, as well as the Department of Energy (DOE) must move to update its energy sector specific plans to protect against future attacks.

While I applaud some of the initiative some electric power companies are taking to protect their facilities, the essential nature of our electric infrastructure to every aspect of our way of life calls for stronger mandatory and enforceable standards at the federal level.

Thank you for your attention to this matter. Please don't hesitate to contact me or my staff should you have any questions.

Sincerely,



Charles E. Schumer
U.S. Senator

Federal Energy Regulatory Commission
Correspondence Control Sheet Report
(Sorted by Document Number)

Document No: 2014-00008

Signature: LaFleur, Cheryl

Priority:	Regular	Via:	E-mail	Date of Document :	02/17/2014
Type :	Electric	Form :	Letter	Date Received :	02/18/2014
Reply :	Yes	Origin :	Incoming	Date Due :	03/07/2014

Authors Name	Company & Title		
Schumer, Charles	Senator	U.S. Senate	NY

Subject : bulk power system; security

Dockets :

Class : Congressional

Infocopy : Moeller Norris LaFleur Clark

Notes: No applicable notes.

Name:	Action:	Due Date:	Office:	Date Completed:	Initials:
[redacted]		02/28/2014	Administration & Operations Staff		

[redacted] [redacted]

From: Michael Bardee
Sent: Tuesday, February 25, 2014 1:50 PM
To: Edward Franks; [redacted]
Subject: Fwd: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)
Attachments: 2014-00015.pdf; control sheet.pdf

Ted: have you seen this yet? We need to assign to someone, for quick turnaround.

- Mike

Sent from my iPad

Begin forwarded message:

From: [redacted]
Date: February 25, 2014 at 11:55:06 AM EST
To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring <Andrea.Spring@ferc.gov>, Andrew Weinstein <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>, David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>, Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>, John Peschke <john.peschke@ferc.gov>, Joshua Konecni <Joshua.Konecni@ferc.gov>, Kim Shannon <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura Vendetta <laura.vendetta@ferc.gov>, Leonard Tao <leonard.tao@ferc.gov>, "Mary O'Driscoll" <Mary.O'Driscoll@ferc.gov>, Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee <Michael.Bardee@ferc.gov>, Nicholas Tackett <nicholas.tackett@ferc.gov>, Patricia Herrion <Patricia.Herrion@ferc.gov>, Robert Ivanauskas <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks <russell.fairbanks@ferc.gov>, Sandra Waldstein <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>, Shawn Bennett <Shawn.Bennett@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
Cc: [redacted] [redacted] Craig Cano <craig.cano@ferc.gov>
Subject: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)

FOR YOUR INFORMATION ONLY.

DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR BEFORE 03/04/14.

--

[redacted]
Staff Assistant
Office of External Affairs
[redacted]

JIM BRIDENSTINE
1ST DISTRICT, OKLAHOMA

216 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2211

2448 EAST 81ST STREET, SUITE 5150
TULSA, OKLAHOMA 74137
(918) 935-3222

Congress of the United States
House of Representatives
Washington, DC 20515-3601

COMMITTEE ON ARMED SERVICES

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY

Bridenstine.House.gov

Facebook.com/CongressmanJimBridenstine
Twitter.com/RepJBridenstine

February 12, 2014

Cheryl LaFleur
Acting Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Acting Commission LaFleur,

Like all Americans, my constituents in Oklahoma's First District rely on a safe and secure electric grid to function in our society. Therefore, I was troubled by a recent article in the *Wall Street Journal* (attached) describing an attack on a San Jose, California-based electrical substation. According to the *Journal*'s reporting, the Metcalf PG&E substation was attacked on April 16, 2013. The attackers subjected the Metcalf facility to a seemingly coordinated and sophisticated sniper attack. Indeed, the former Chairman of the Federal Energy Regulatory Commission (FERC), Jon Wellinghoff, described the attack as "domestic terrorism."

The Metcalf attack demonstrates the vulnerability of our electric grid, specifically its vital components that remain too easily exposed to physical attacks. As a Member of the House Armed Services Committee, I listed to frequent testimony from our military leadership regarding the consequences of cyberattack on this nation's critical infrastructure. The Metcalf shows that physical security is still very important even though cyber is much more in the news. I am concerned that the grid remains too vulnerable from a physical protection perspective.

According to the *Journal*, the FBI has made no arrests in the case. I request an update on the FBI's investigation into this matter. I would also like your assessment regarding whether or not this attack qualifies as "domestic terrorism". My staff member on this matter is James Mazol (james.mazol@mail.house.gov).

Sincerely,

Jim Bridenstine

2014-00015

Assault on California Power Station Raises Alarm on Potential for Terrorism

April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid

Feb. 4, 2014 10:30 p.m. ET

SAN JOSE, Calif.—The attack began just before 1 a.m. on April 16 last year, when someone slipped into an underground vault not far from a busy freeway and cut telephone cables.

Within half an hour, snipers opened fire on a nearby electrical substation. Shooting for 19 minutes, they surgically knocked out 17 giant transformers that funnel power to Silicon Valley. A minute before a police car arrived, the shooters disappeared into the night.

A sniper attack in April that knocked out an electrical substation near San Jose, Calif., has raised fears that the country's power grid is vulnerable to terrorism. WSJ's Rebecca Smith has the details. Photo: Talia Herman for The Wall Street Journal

With over 160,000 miles of transmission lines, the U.S. power grid is designed to handle natural and man-made disasters, as well as fluctuations in demand. How does the system work? WSJ's Jason Bellini has #TheShortAnswer.

To avoid a blackout, electric-grid officials rerouted power around the site and asked power plants in Silicon Valley to produce more electricity. But it took utility workers 27 days to make repairs and bring the substation back to life.

Nobody has been arrested or charged in the attack at PG&E Corp.'s PCG +0.09% PG&E Corp. U.S.: NYSE $42.48 +0.04 +0.09% Feb. 12, 2014 9:40 am Volume (Delayed 15m) : 0 P/E Ratio 26.21 Market Cap $19.07 Billion Dividend Yield 4.29% Rev. per Employee $757,442 02/11/14 PG&E swings to profit with few... 02/09/14 U.S. Utilities Tighten Securit... 02/05/14 Q&A: What You Need to Know Abo... More quote details and news » PCG in Your Value Your Change Short position Metcalf transmission substation. It is an incident of which few Americans are aware. But one former federal regulator is calling it a terrorist act that, if it were widely replicated across the country, could take down the U.S. electric grid and black out much of the country.

The attack was "the most significant incident of domestic terrorism involving the grid that has ever occurred" in the U.S., said Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time.

The Wall Street Journal assembled a chronology of the Metcalf attack from filings PG&E made to state and federal regulators; from other documents including a video released by the Santa Clara County Sheriff's Department; and from interviews, including with Mr. Wellinghoff.

Related

Q&A: What You Need to Know About Attacks on the U.S. Power Grid

The 64-year-old Nevadan, who was appointed to FERC in 2006 by President George W. Bush and stepped down in November, said he gave closed-door, high-level briefings to federal agencies, Congress and the White House last year. As months have passed without arrests, he said, he has grown increasingly concerned that an even larger attack could be in the works. He said he was going public about the incident out of concern that national security is at risk and critical electric-grid sites aren't adequately protected.

The Federal Bureau of Investigation doesn't think a terrorist organization caused the Metcalf attack, said a spokesman for the FBI in San Francisco. Investigators are "continuing to sift through the evidence," he said.

Some people in the utility industry share Mr. Wellinghoff's concerns, including a former official at PG&E, Metcalf's owner, who told an industry gathering in November he feared the incident could have been a dress rehearsal for a larger event.

"This wasn't an incident where Billy-Bob and Joe decided, after a few brewskis, to come in and shoot up a substation," Mark Johnson, retired vice president of transmission for PG&E, told the utility security conference, according to a video of his presentation. "This was an event that was well thought out, well planned and they targeted certain components." When reached, Mr. Johnson declined to comment further.

A spokesman for PG&E said the company takes all incidents seriously but declined to discuss the Metcalf event in detail for fear of giving information to potential copycats. "We won't speculate about the motives" of the attackers, added the spokesman, Brian Swanson. He said PG&E has increased security measures.

Utility executives and federal energy officials have long worried that the electric grid is vulnerable to sabotage. That is in part because the grid, which is really three systems serving different areas of the U.S., has failed when small problems such as trees hitting transmission lines created cascading blackouts. One in 2003 knocked out power to 50 million people in the Eastern U.S. and Canada for days.

Many of the system's most important components sit out in the open, often in remote locations, protected by little more than cameras and chain-link fences.

Transmission substations are critical links in the grid. They make it possible for electricity to move long distances, and serve as hubs for intersecting power lines.

Within a substation, transformers raise the voltage of electricity so it can travel hundreds of miles on high-voltage lines, or reduce voltages when electricity approaches its destination. The Metcalf substation functions as an off-ramp from power lines for electricity heading to homes and businesses in Silicon Valley.

The country's roughly 2,000 very large transformers are expensive to build, often costing millions of dollars each, and hard to replace. Each is custom made and weighs up to 500,000 pounds, and "I can only build 10 units a month," said Dennis Blake, general manager of Pennsylvania Transformer in Pittsburgh, one of seven U.S. manufacturers. The utility industry keeps some spares on hand.

A 2009 Energy Department report said that "physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale...could result in prolonged outages, as procurement cycles for these components range from months to years."

Mr. Wellinghoff said a FERC analysis found that if a surprisingly small number of U.S. substations were knocked out at once, that could destabilize the system enough to cause a blackout that could encompass most of the U.S.

Not everyone is so pessimistic. Gerry Cauley, chief executive of the North America Electric Reliability Corp., a standards-setting group that reports to FERC, said he thinks the grid is more resilient than Mr. Wellinghoff fears.

"I don't want to downplay the scenario he describes," Mr. Cauley said. "I'll agree it's possible from a technical assessment." But he said that even if several substations went down, the vast majority of people would have their power back in a few hours.

The utility industry has been focused on Internet attacks, worrying that hackers could take down the grid by disabling communications and important pieces of equipment. Companies have reported 13 cyber incidents in the past three years, according to a Wall Street Journal analysis of emergency reports utilities file with the federal government. There have been no reports of major outages linked to these events, although companies have generally declined to provide details.

"A lot of people in the electric industry have been distracted by cybersecurity threats," said Stephen Berberich, chief executive of the California Independent System Operator, which runs much of the high-voltage transmission system for the utilities. He said that physical attacks pose a "big, if not bigger" menace.

There were 274 significant instances of vandalism or deliberate damage in the three years, and more than 700 weather-related problems, according to the Journal's analysis.

Until the Metcalf incident, attacks on U.S. utility equipment were mostly linked to metal thieves, disgruntled employees or bored hunters, who sometimes took potshots at small transformers on utility poles to see what happens. (Answer: a small explosion followed by an outage.)

Last year, an Arkansas man was charged with multiple attacks on the power grid, including setting fire to a switching station. He has pleaded not guilty and is undergoing a psychiatric evaluation, according to federal court records.

Overseas, terrorist organizations were linked to 2,500 attacks on transmission lines or towers and at least 500 on substations from 1996 to 2006, according to a January report from the Electric Power Research Institute, an industry-funded research group, which cited State Department data.

An attack on a PG&E substation near San Jose, Calif., in April knocked out 17 transformers like this one. Talia Herman for The Wall Street Journal

To some, the Metcalf incident has lifted the discussion of serious U.S. grid attacks beyond the theoretical. "The breadth and depth of the attack was unprecedented" in the U.S., said Rich Lordan, senior technical executive for the Electric Power Research Institute. The motivation, he said, "appears to be preparation for an act of war."

The attack lasted slightly less than an hour, according to the chronology assembled by the Journal.

At 12:58 a.m., AT&T fiber-optic telecommunications cables were cut—in a way that made them hard to repair—in an underground vault near the substation, not far from U.S. Highway 101 just outside south San Jose. It would have taken more than one person to lift the metal vault cover, said people who visited the site.

Nine minutes later, some customers of Level 3 Communications, LVLT +0.35% Level 3 Communications Inc. U.S.: NYSE $36.83 +0.13 +0.35% Feb. 12, 2014 9:39 am Volume (Delayed 15m) : 0 P/E Ratio N/A Market Cap $8.21 Billion Dividend Yield N/A Rev. per Employee $584,537 02/05/14 Level 3 Swings to Profit on Lo... 01/27/14 Puzzle for CFOs: Fixed or Floa... 11/26/13 The Morning Download: NSA Reve... More quote details and news » LVLT in Your Value Your Change Short position an Internet service provider, lost service. Cables in its vault near the Metcalf substation were also cut.

At 1:31 a.m., a surveillance camera pointed along a chain-link fence around the substation recorded a streak of light that investigators from the Santa Clara County Sheriff's office think was a signal from a waved flashlight. It was followed by the muzzle flash of rifles and sparks from bullets hitting the fence.

The substation's cameras weren't aimed outside its perimeter, where the attackers were. They shooters appear to have aimed at the transformers' oil-filled cooling systems. These began to bleed oil, but didn't explode, as the transformers probably would have done if hit in other areas.

About six minutes after the shooting started, PG&E confirms, it got an alarm from motion sensors at the substation, possibly from bullets grazing the fence, which is shown on video.

Four minutes later, at 1:41 a.m., the sheriff's department received a 911 call about gunfire, sent by an engineer at a nearby power plant that still had phone service.

Riddled with bullet holes, the transformers leaked 52,000 gallons of oil, then overheated. The first bank of them crashed at 1:45 a.m., at which time PG&E's control center about 90 miles north received an equipment-failure alarm.

Five minutes later, another apparent flashlight signal, caught on film, marked the end of the attack. More than 100 shell casings of the sort ejected by AK-47s were later found at the site.

At 1:51 a.m., law-enforcement officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.

A PG&E worker, awakened by the utility's control center at 2:03 a.m., arrived at 3:15 a.m. to survey the damage.

Grid officials routed some power around the substation to keep the system stable and asked customers in Silicon Valley to conserve electricity.

In a news release, PG&E said the substation had been hit by vandals. It has since confirmed 17 transformers were knocked out.

Mr. Wellinghoff, then chairman of FERC, said that after he heard about the scope of the attack, he flew to California, bringing with him experts from the U.S. Navy's Dahlgren Surface Warfare Center in Virginia, which trains Navy SEALs. After walking the site with PG&E officials and FBI agents, Mr. Wellinghoff said, the military experts told him it looked like a professional job.

In addition to fingerprint-free shell casings, they pointed out small piles of rocks, which they said could have been left by an advance scout to tell the attackers where to get the best shots.

"They said it was a targeting package just like they would put together for an attack," Mr. Wellinghoff said.

Mr. Wellinghoff, now a law partner at Stoel Rives LLP in San Francisco, said he arranged a series of meetings in the following weeks to let other federal agencies, including the Department of Homeland Security, know what happened and to enlist their help. He held a closed-door meeting with utility executives in San Francisco in June and has distributed lists of things utilities should do to strengthen their defenses.

A spokesman for Homeland Security said it is up to utilities to protect the grid. The department's role in an emergency is to connect federal agencies and local police and facilitate information sharing, the spokesman said.

As word of the attack spread through the utility industry, some companies moved swiftly to review their security efforts. "We're looking at things differently now," said Michelle Campanella, an FBI veteran who is director of security for Consolidated Edison Inc. ED -0.99% Consolidated Edison Inc. U.S.: NYSE $53.89 -0.54 -0.99% Feb. 12, 2014 9:40 am Volume (Delayed 15m) : 0 P/E Ratio 15.38 Market Cap $15.94 Billion Dividend Yield 4.63% Rev. per Employee $852,158 01/14/14 Con Ed Rates, Frozen For Now, ... More quote details and news » ED in Your Value Your Change Short position in New York. For example, she said, Con Ed changed the angles of some of its 1,200 security cameras "so we don't have any blind spots."

Some of the legislators Mr. Wellinghoff briefed are calling for action. Rep. Henry Waxman (D., Calif.) mentioned the incident at a FERC oversight hearing in December, saying he was concerned that no one in government can order utilities to improve grid protections or to take charge in an emergency.

As for Mr. Wellinghoff, he said he has made something of a hobby of visiting big substations to look over defenses and see whether he is questioned by security details or local police. He said he typically finds easy access to fence lines that are often close to important equipment.

"What keeps me awake at night is a physical attack that could take down the grid," he said. "This is a huge problem."

—Tom McGinty contributed to this article.

Write to Rebecca Smith at rebecca.smith@wsj.com

Federal Energy Regulatory Commission
Correspondence Control Sheet Report
(Sorted by Document Number)

2/25/2014
11:29:45AM

Document No: 2014-00015

Signature: LaFleur, Cheryl

Priority:	Regular	Via:	Mail	Date of Document :	02/12/2014
Type :	Electric	Form :	Letter	Date Received :	02/25/2014
Reply :	Yes	Origin :	Incoming	Date Due :	03/11/2014

Authors Name	Company & Title		
Bridenstine, Jim	Congressman	US House	OK

Subject : bulk power system; security

Dockets :

Class : Congressional

Infocopy : Moeller Norris LaFleur Clark

Notes: No applicable notes.

Name:	Action:	Due Date:	Office:	Date Completed:	Initials:
[redacted]	Assignment	03/04/2014	Administration & Operations Staff		

[redacted] [redacted]

From: Michael Bardee
Sent: Wednesday, March 12, 2014 9:48 PM
To: James P. Fama (jfama@eei.org); Lawson, Barry R.; Mosher, Allen; bhindin@eei.org; jonathan.schneider@stinsonleonard.com
Subject: Wall Street Journal article
Attachments: WSJ-03-12-14 (4).pdf

FYI.

THE WALL STREET JOURNAL.
BUSINESS

U.S. Risks National Blackout From Small-Scale Attack

Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

By REBECCA SMITH

March 12, 2014 7:03 p.m. ET

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.

A small number of the country's substations play an outsize role in keeping power flowing across large regions. The FERC analysis indicates that knocking out nine of those key substations could plunge the country into darkness for weeks, if not months.

"This would be an event of unprecedented proportions," said Ross Baldick, a professor of electrical engineering at the University of Texas at Austin.

No federal rules require utilities to protect vital substations except those at nuclear power plants. Regulators recently said they would consider imposing security standards.

FERC last year used software to model the electric system's performance under the stress of losing important substations. The substations use large power transformers to boost the voltage of electricity so it can move long distances and then to reduce the voltage to a usable level as the electricity nears homes and businesses.

The agency's so-called power-flow analysis found that different sets of nine big substations produced similar results. The Wall Street Journal isn't publishing the list of 30 critical substations studied by FERC. The commission declined to discuss the analysis or to release its contents.

Some federal officials said the conclusions might overstate the grid's vulnerability.

Electric systems are designed to be resilient and it would be difficult for attackers to disable many locations, said David Ortiz, an Energy Department deputy assistant secretary who was briefed on the FERC study. The agency's findings nevertheless had value "as a way of starting a conversation on physical security," he said.

reported by the Journal last month, Mr. Wellinghoff was concerned about a shooting attack on a California substation last April, which he said could be a dress rehearsal for additional assaults.

"There are probably less than 100 critical high voltage substations on our grid in this country that need to be protected from a physical attack," he said by email this week. "It is neither a monumental task, nor is it an inordinate sum of money that would be required to do so." Mr. Wellinghoff left FERC in November and is a partner at law firm Stoel Rives LLP in San Francisco.

FERC has given the industry until early June to propose new standards for the security of critical facilities, such as substations.

Executives at several big utilities declined to discuss the risks to substations but said they are increasing spending on security. Virginia-based Dominion Resources Inc., for example, said it planned to spend $300 million to $500 million within seven years to harden its facilities.

A memo prepared at FERC in late June for Mr. Wellinghoff before he briefed senior officials made several urgent points. "Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," said the memo, which was reviewed by the Journal. That lengthy outage is possible for several reasons, including that only a handful of U.S. factories build transformers.

The California attack "demonstrates that it does not require sophistication to do significant damage to the U.S. grid," according to the memo, which was written by Leonard Tao, FERC's director of external affairs. Mr. Tao said his function was to help Mr. Wellinghoff simplify his report on the analysis.

The memo reflected a belief by some people at the agency that an attack-related blackout could be extraordinarily long, in part because big transformers and other equipment are hard to replace. Also, each of the three regional electric systems—the West, the East and Texas—have limited interconnections, making it hard for them to help each other in an emergency.

Some experts said other simulations that are widely used in the electricity industry produced similar results as the FERC analysis.

"This study used a relatively simplified model, but other models come to the same conclusion," said A.P. "Sakis" Meliopoulos, professor of electrical and computer engineering at the Georgia Institute of Technology in Atlanta. He estimated it would take "a slightly larger number" of substation attacks to cause a U.S.-wide blackout.

In its modeling, FERC studied what would happen if various combinations of substations were crippled in the three electrical systems that serve the contiguous U.S. The agency concluded the systems could go dark if as few as nine locations were knocked out: four in the East, three the West and two in Texas, people with knowledge of the analysis said.

The actual number of locations that would have to be knocked out to spawn a massive blackout would vary depending on available generation resources, energy demand, which is highest on hot days, and other factors, experts said. Because it is difficult to build new transmission routes, existing big substations are becoming more crucial to handling electricity.

The Metcalf substation sits near a freeway outside San Jose, Calif. Some experts worry that substations farther from cities could face longer attacks because of their distance from police. Many sites aren't staffed and are protected by little more than chain-link fences and cameras.

While the prospect of a nationwide blackout because of sabotage might seem remote, small equipment failures have led to widespread power outages. In September 2011, for example, a failed transmission line in Arizona set off a chain reaction that created an outage affecting millions of people in the state and Southern California.

Sabotage could wreak worse havoc, experts said.

"The power grid, built over many decades in a benign environment, now faces a range of threats it was never designed to survive," said Paul Stockton, a former assistant secretary of defense and president of risk-assessment firm Cloud Peak Analytics. "That's got to be the focus going forward."

Write to Rebecca Smith at rebecca.smith@wsj.com

[redacted]

From: Michael Bardee
Sent: Thursday, March 13, 2014 4:09 AM
To: Edward Franks; David Andrejcak; Keith O'Neal; Mark Hegerle
Subject: Fwd: Wall Street Journal Article
Attachments: image001.gif; image002.gif; image003.gif; image004.gif; WSJ-03-12-14.pdf

FYI.

Sent from my iPad

Begin forwarded message:

> **From:** Diane Bernier2 <diane.bernier@ferc.gov>
> **Date:** March 12, 2014 at 8:12:06 PM EDT
> **To:** ArticleDL <articledl@ferc.gov>
> **Subject: Wall Street Journal Article**
>
> Please see attached. Article came out within the past hour.
>
> *Diane E. Bernier*
> Office of External Affairs | Media Relations
> Federal Energy Regulatory Commission
> Phone: 202-502-6109
> Toll Free: 1-866-208-3372

THE WALL STREET JOURNAL.

BUSINESS

U.S. Risks National Blackout From Small-Scale Attack

Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

By REBECCA SMITH

March 12, 2014 7:03 p.m. ET

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.

A small number of the country's substations play an outsize role in keeping power flowing across large regions. The FERC analysis indicates that knocking out nine of those key substations could plunge the country into darkness for weeks, if not months.

"This would be an event of unprecedented proportions," said Ross Baldick, a professor of electrical engineering at the University of Texas at Austin.

No federal rules require utilities to protect vital substations except those at nuclear power plants. Regulators recently said they would consider imposing security standards.

FERC last year used software to model the electric system's performance under the stress of losing important substations. The substations use large power transformers to boost the voltage of electricity so it can move long distances and then to reduce the voltage to a usable level as the electricity nears homes and businesses.

The agency's so-called power-flow analysis found that different sets of nine big substations produced similar results. The Wall Street Journal isn't publishing the list of 30 critical substations studied by FERC. The commission declined to discuss the analysis or to release its contents.

Some federal officials said the conclusions might overstate the grid's vulnerability.

Electric systems are designed to be resilient and it would be difficult for attackers to disable many locations, said David Ortiz, an Energy Department deputy assistant secretary who was briefed on the FERC study. The agency's findings nevertheless had value "as a way of starting a conversation on physical security," he said.

reported by the Journal last month, Mr. Wellinghoff was concerned about a shooting attack on a California substation last April, which he said could be a dress rehearsal for additional assaults.

"There are probably less than 100 critical high voltage substations on our grid in this country that need to be protected from a physical attack," he said by email this week. "It is neither a monumental task, nor is it an inordinate sum of money that would be required to do so." Mr. Wellinghoff left FERC in November and is a partner at law firm Stoel Rives LLP in San Francisco.

FERC has given the industry until early June to propose new standards for the security of critical facilities, such as substations.

Executives at several big utilities declined to discuss the risks to substations but said they are increasing spending on security. Virginia-based Dominion Resources Inc., for example, said it planned to spend $300 million to $500 million within seven years to harden its facilities.

A memo prepared at FERC in late June for Mr. Wellinghoff before he briefed senior officials made several urgent points. "Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," said the memo, which was reviewed by the Journal. That lengthy outage is possible for several reasons, including that only a handful of U.S. factories build transformers.

The California attack "demonstrates that it does not require sophistication to do significant damage to the U.S. grid," according to the memo, which was written by Leonard Tao, FERC's director of external affairs. Mr. Tao said his function was to help Mr. Wellinghoff simplify his report on the analysis.

The memo reflected a belief by some people at the agency that an attack-related blackout could be extraordinarily long, in part because big transformers and other equipment are hard to replace. Also, each of the three regional electric systems—the West, the East and Texas—have limited interconnections, making it hard for them to help each other in an emergency.

Some experts said other simulations that are widely used in the electricity industry produced similar results as the FERC analysis.

"This study used a relatively simplified model, but other models come to the same conclusion," said A.P. "Sakis" Meliopoulos, professor of electrical and computer engineering at the Georgia Institute of Technology in Atlanta. He estimated it would take "a slightly larger number" of substation attacks to cause a U.S.-wide blackout.

In its modeling, FERC studied what would happen if various combinations of substations were crippled in the three electrical systems that serve the contiguous U.S. The agency concluded the systems could go dark if as few as nine locations were knocked out: four in the East, three the West and two in Texas, people with knowledge of the analysis said.

The actual number of locations that would have to be knocked out to spawn a massive blackout would vary depending on available generation resources, energy demand, which is highest on hot days, and other factors, experts said. Because it is difficult to build new transmission routes, existing big substations are becoming more crucial to handling electricity.

The Metcalf substation sits near a freeway outside San Jose, Calif. Some experts worry that substations farther from cities could face longer attacks because of their distance from police. Many sites aren't staffed and are protected by little more than chain-link fences and cameras.

While the prospect of a nationwide blackout because of sabotage might seem remote, small equipment failures have led to widespread power outages. In September 2011, for example, a failed transmission line in Arizona set off a chain reaction that created an outage affecting millions of people in the state and Southern California.

Sabotage could wreak worse havoc, experts said.

"The power grid, built over many decades in a benign environment, now faces a range of threats it was never designed to survive," said Paul Stockton, a former assistant secretary of defense and president of risk-assessment firm Cloud Peak Analytics. "That's got to be the focus going forward."

Write to Rebecca Smith at rebecca.smith@wsj.com

[redacted] [redacted]

From: Michael Bardee
Sent: Friday, April 04, 2014 1:40 PM
To: Jehmal Hudson
Cc: Joseph McClelland; [redacted] Edward Franks; David Morenoff; Christy Walsh; Martin Kirkwood; Leonard Tao; Chris Murray; Andrea Spring
Subject: Re: FERC Briefing - Congressman Pittenger

That works for me, Jehmal. Thanks.

- Mike

On Fri, Apr 4, 2014 at 11:59 AM, Jehmal Hudson <jehmal.hudson@ferc.gov> wrote:
Congressman Pittenger's (R-TX) office has requested a briefing on the vulnerabilities to the electric grid. After speaking to his staffer, the Congressman would like to focus on EMP/GMD issues, physcial security (Metcalf) and protecting infrastructure from vulnerabilities and threats. The meeting will just be with the Congressman and his staffer and no other Members.

Tentatively, the Congressman would like for us to come in on Wednesday, April 30 at 2:00pm. Would that work for everyone?

Thanks,
Jehmal

---------- Forwarded message ----------
From: **Billy, Stephen** <Stephen.Billy@mail.house.gov>
Date: Thu, Apr 3, 2014 at 5:07 PM
Subject: FERC Briefing - Congressman Pittenger
To: "jehmal.hudson@ferc.gov" <jehmal.hudson@ferc.gov>
Cc: "Wall, Erin" <erin.wall@mail.house.gov>

Jehmal –

Appreciate your help in setting this up. I've looped in Erin Wall from our office to help set a date and time.

As we discussed on the phone, Congressman Pittenger is interested in a briefing on where our country is currently as far as vulnerabilities in our infrastructure. I think it makes sense, giving some previous conversations he has had, to start with the electric grid and EMP and disruptions generally (such as the one in California last year). Moving forward, I know the Congressman will be interested in discussing water and energy supply vulnerabilities too.

Just some quick background, Congressman Pittenger is coming at this issue from the view as the Chairman of the Congressional Taskforce on Terrorism and Unconventional Warfare. Really he is at a stage where he wants to just get as much information as possible and make sure he and the taskforce have a firm understanding of the issues they are dealing with. There is no plan for any legislative action or anything of that nature, this is just more of a fact finding briefing to familiarize the Members with the possible problems and solutions.

Thanks for the help!

Regards,

Stephen Billy

Legislative Assistant

Office of Congressman Robert Pittenger (R-NC)

224 Cannon House Office Building

(202) 225-1976

--

Jehmal Terrence Hudson, Esq.

House Congressional Liaison

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6142

Jehmal.Hudson@ferc.gov

Follow us on Twitter & Facebook

[redacted]

From: Michael Bardee
Sent: Tuesday, May 13, 2014 8:24 PM
To: [redacted]
Subject: Fwd: I/C (Rep. Lofgren) large power transformers and electric grids; security (2014-00115)
Attachments: 2014-00115.pdf; control sheet.pdf

[redacted] despite the reference to OEMR below, subsequent emails between office directors have given this assignment to OER. Do you have someone in your group who can draft a reply in the next day or two? I can give you a copy of some recent answers to other questions that will help, and can discuss in the morning.

- Mike

---------- Forwarded message ----------
From: [redacted]
Date: Tue, May 13, 2014 at 3:56 PM
Subject: I/C (Rep. Lofgren) large power transformers and electric grids; security (2014-00115)
To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring <Andrea.Spring@ferc.gov>, Andrew Weinstein <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>, David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>, Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>, John Peschke <john.peschke@ferc.gov>, Kim Shannon <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura Vendetta <laura.vendetta@ferc.gov>, Leonard Tao <leonard.tao@ferc.gov>, Mary O'Driscoll <Mary.O'Driscoll@ferc.gov>, Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee <Michael.Bardee@ferc.gov>, Nicholas Tackett <nicholas.tackett@ferc.gov>, Patricia Herrion <Patricia.Herrion@ferc.gov>, Robert Ivanauskas <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks <russell.fairbanks@ferc.gov>, Sandra Waldstein <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>, Shawn Bennett <Shawn.Bennett@ferc.gov>, Steven Wellner <steven.wellner@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
Cc: [redacted] Craig Cano <craig.cano@ferc.gov>

FOR YOUR INFORMATION ONLY.

DOCUMENT ASSIGNED TO OEMR FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR BEFORE 05/20/14.

--

[redacted]
Office of External Affairs
[redacted]

COMMITTEE ON THE JUDICIARY
•RANKING MEMBER-SUBCOMMITTEE ON IMMIGRATION AND BORDER SECURITY
•SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY AND THE INTERNET

COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
•SUBCOMMITTEE ON ENERGY
•SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

COMMITTEE ON HOUSE ADMINISTRATION
•JOINT COMMITTEE ON THE LIBRARY

Congress of the United States
House of Representatives
Washington, DC 20515

ZOE LOFGREN
19TH DISTRICT, CALIFORNIA

635 NORTH FIRST STREET
SUITE B
SAN JOSE, CA 95112
(408) 271-8700

1401 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3072

LOFGREN.HOUSE.GOV

CHAIR, CALIFORNIA DEMOCRATIC CONGRESSIONAL DELEGATION

CO-CHAIR, CONGRESSIONAL CAUCUS ON VIETNAM

The Honorable Cheryl A. LaFleur
Acting Chairman
Federal Energy Regulatory Commission
888 1st Street NE
Washington, D.C. 20426

May 12, 2014

Dear Chairman LaFleur,

I am writing with regard to the Department of Energy (DOE)'s April 2014 update to its report "Large Power Transformers and the U.S. Electric Grid" ("LPT report").

As you are aware, last April, an attack occurred at PG&E's Metcalf substation, located in the 19th Congressional District of California, which I represent. The attack damaged 17 transformers, requiring power to be rerouted and other area power plants to generate additional electricity. Although outages were avoided, had this attack occurred during peak season, I understand that rolling blackouts would have occurred throughout our region. The San Francisco Bay Area has an economic productivity almost twice the national average, contains more Fortune 500 companies than any other U.S. region outside of New York, and generates the most patents in the country. A successfully executed attack on our infrastructure would have not only regional consequences, but national implications.

I have attended a number of briefings on the Metcalf incident in which the availability of spare transformers and the lead time required for manufacturing new transformers have been discussed. At a recent closed-door briefing hosted by the Energy and Commerce Committee, presented by representatives from FERC, DOE, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and a number of utilities, [redacted]

However, according to the LPT report, a number of concerns remain, including:

- LPTs are usually neither interchangeable with one another nor produced for extensive spare inventories – in fact, only approximately 1.3 transformers are produced for each transformer design
- The U.S. has limited capability to manufacture LPTs. In 2010, only 15 percent of U.S. demand for transformers was met through domestic production. That same year, the U.S. had only six domestic manufacturers while China had over 30.
- This limited domestic manufacturing capability could present a supply issue if multiple LPTs simultaneously fail.

2014-00115

I would like clarification on whether there are sufficient stockpiles of LPTs, whether efforts are being made to reduce U.S. reliance on foreign LPT manufacturers, and whether it is possible to pursue greater standardization, especially as we look to replace our aging fleet of LPTs. I appreciate your attention to this matter, and look forward to your response.

Sincerely,

Zoe Lofgren
Member of Congress

Federal Energy Regulatory Commission
Correspondence Control Sheet Report
(Sorted by Document Number)

Document No: 2014-00115

	Priority:	Regular	Via:	E-mail	Date of Document : 05/12/2014
Signature: LaFleur, Cheryl	Type :	Electric	Form :	Letter	Date Received : 05/13/2014
	Reply :	Yes	Origin :	Incoming	Date Due : 05/27/2014

Authors Name	**Company & Title**	
Lofgren, Zoe	Congressman	U.S. House CA

Subject : large power transformers and electric grids; security

Dockets :

Class : Congressional

Infocopy : Moeller Norris LaFleur Clark

Notes: No applicable notes.

Name:	Action:	Due Date:	Office:	Date Completed:	Initials:
[redacted]	Assignment	05/20/2014	Administration And Operations Staff		

[redacted]

From: Michael Bardee
Sent: Thursday, May 15, 2014 12:08 PM
To: David Morenoff
Cc: Jehmal Hudson; [redacted] Leonard Tao; Chris Murray; Andrea Spring; Joseph McClelland; Edward Franks; Christy Walsh; Martin Kirkwood
Subject: Re: FERC briefing - Congressman Pittenger

[redacted]

On Thu, May 15, 2014 at 12:00 PM, David Morenoff <david.morenoff@ferc.gov> wrote:
Jehmal,

I expect that OGC could have an appropriate representative available to attend the meeting on June 11th. We will decide who will cover the meeting depending on what else is scheduled for that morning, including what items are scheduled for discussion at pre-agenda.

Thanks,
David

On Thu, May 15, 2014 at 10:36 AM, Jehmal Hudson <jehmal.hudson@ferc.gov> wrote:
[redacted] Would June 11 be better for folks?

On Thu, May 15, 2014 at 10:33 AM, [redacted] wrote:

Jehmal,

Joe is on travel May 21st. June 11th would work.

Thanks,

[redacted]

From: Jehmal Hudson [mailto:jehmal.hudson@ferc.gov]
Sent: Thursday, May 15, 2014 10:22 AM
To: Joseph McClelland; [redacted] Michael Bardee; Edward Franks; David Morenoff; Christy Walsh; Martin Kirkwood
Cc: Leonard Tao; Chris Murray; Andrea Spring
Subject: FERC briefing - Congressman Pittenger

As you know, Congressman Pittenger (R-TX) recently requested a briefing on the vulnerabilities of the electric grid. Since the Congressman would prefer the freedom to ask questions that might border on issues

such as the Metcalf incident, his staffer has located some possible dates and times to book a SCIF. Also to note, Congressman Kennedy (D-MA) will be in attendance.

Presently, below are the following dates that works on their end:

May 21st 11:30a.m.

June 10th 10:30a.m.- 12:30p.m.

June 11th 9:00a.m.- 12:30p.m.

What is everyone's availability for May 21st at 11:30am?

Thanks,

Jehmal

--

Jehmal Terrence Hudson, Esq.

House Congressional Liaison

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6142

Jehmal.Hudson@ferc.gov

Follow us on Twitter & Facebook

--

Jehmal Terrence Hudson, Esq.

House Congressional Liaison

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6142

Jehmal.Hudson@ferc.gov

Follow us on Twitter & Facebook

[redacted]

From: Michael Bardee
Sent: Wednesday, May 28, 2014 7:49 PM
To: Edward Franks
Subject: Fwd: I/C (Rep. JeffDuncan) bulk power system security, Metcalf station (2014-00129)
Attachments: 2014-00129.pdf; control sheet.pdf

Ted: [redacted]

- Mike

---------- Forwarded message ----------
From: [redacted]
Date: Wed, May 28, 2014 at 5:30 PM
Subject: I/C (Rep. JeffDuncan) bulk power system security, Metcalf station (2014-00129)
To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring <Andrea.Spring@ferc.gov>, Andrew Weinstein <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>, David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>, Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>, John Peschke <john.peschke@ferc.gov>, Kim Shannon <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura Vendetta <laura.vendetta@ferc.gov>, Leonard Tao <leonard.tao@ferc.gov>, Mary O'Driscoll <Mary.O'Driscoll@ferc.gov>, Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee <Michael.Bardee@ferc.gov>, Nicholas Tackett <nicholas.tackett@ferc.gov>, Patricia Herrion <Patricia.Herrion@ferc.gov>, Robert Ivanauskas <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks <russell.fairbanks@ferc.gov>, Sandra Waldstein <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>, Shawn Bennett <Shawn.Bennett@ferc.gov>, Steven Wellner <steven.wellner@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
Cc: [redacted] Craig Cano <craig.cano@ferc.gov>

FOR YOUR INFORMATION ONLY.

DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR BEFORE 06/05/14.

--

[redacted]
Office of External Affairs
[redacted]

JEFF DUNCAN
3RD DISTRICT, SOUTH CAROLINA

COMMITTEE ON HOMELAND SECURITY
CHAIRMAN
SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

COMMITTEE ON NATURAL RESOURCES

COMMITTEE ON FOREIGN AFFAIRS

NON-DOCKETED ITEM

Congress of the United States

House of Representatives

Washington, DC 20515-4003

116 CANNON HOUSE OFFICE BUILDING
WASHINGTON, D.C. 20515
PHONE: 202.225.5301

303 WEST BELTLINE BOULEVARD
ANDERSON, SC 29625
(864)224-7401

200 COURTHOUSE PUBLIC SQUARE
LAURENS, SC 29360
(864)681-1028

jeffduncan.house.gov

April 28, 2014

RE: Roy Mendelsohn

Dear Mr. Hudson,

I have been contacted by the above-named constituent regarding the status of a response to his letter dated February 12, 2014. The letter in question is attached.

Thank you for your cooperation in this matter.

Blessings and Liberty,

Jeff Duncan
Member of Congress

Click here to get updates on important issues sent directly to your email address.

Please do not reply to this email. The mailbox is unattended.
To share your thoughts please visit my webpage.

Ms. Jordan Sherer

Constituent Liaison/District Scheduler

Office of Congressman Jeff Duncan, SC-3

303 West Beltline Blvd.

Anderson, SC 29625

Office: (864) 224-7401

Fax: (864) 225-7049

2014-00129

1131 Summerset Bay Drive
Cross Hill, SC 29332

Mr. Jon Wellinghoff, Chairman
Federal Energy Regulatory Commission
Washington, DC 20426

February 12, 2014

Dear Mr. Wellinghoff,

I watched your interview on PBS News Hour last night (2/11/14) and was appalled that you would publicly discuss the vulnerability of the nation's power system. This information must have been of great value to those who would do our nation harm, including international terrorists and domestic vandals. They will now be aware that most of our substations are protected only by chain link fences with powerful transformers susceptible to high powered rifles fired from a safe distance.

As a constructor, I have been involved in power projects, hydro, fossil and nuclear, and am well aware of the safety requirements for these projects. I was not aware of the apparent vulnerability of the transmission infrastructure. Now I am, along with three quarters of the planet, well aware of this vulnerability, thanks to the information you so freely disseminated on television.

In other correspondence I have had with you and the FERC, I have complained loudly about the overwhelming and suffocating regulatory regime that the FERC imposes on the power industry. Given your remarks that the vulnerability of our power grid infrastructure requires national attention and federal control, it seems you are seeking to impose extended FERC oversight and control and a substantial increase in the bureaucratic burden carried by the power industry, together with a substantial increase in the cost of power to every citizen.

Given that bureaucracies never cease to expand their control and influence, perhaps this was your motive in appearing on the PBS News Hour. You may well be successful. However, you may find yourself presiding over an industry suffering from widespread attacks and damage thanks to the information you made so freely and widely available to those who would do us harm.

I am copying this letter to my Congressman and Senator with a request that Congress convene committees to establish adequate protective measures and to divert any expansion of the FERC's already excessive regulation of the power industry.

Respectfully yours,

Roy Mendelsohn

Copy to: Senator Tim Scott
Congressman Jeff Duncan

Federal Energy Regulatory Commission
Correspondence Control Sheet Report
(Sorted by Document Number)

Document No: 2014-00129

	Priority: Regular	Via: E-mail	Date of Document:	04/28/2014
Signature: LaFleur, Cheryl	Type: Electric	Form: Letter	Date Received:	05/28/2014
	Reply: Yes	Origin: Incoming	Date Due:	06/11/2014

Authors Name	Company & Title		
Duncan, Jeff	Congressman	U.S. House	SC

Subject: bulk power system security; Metcalf station

Dockets:

Class: Congressional Constituent Mail

Infocopy: Moeller Norris LaFleur Clark

Notes: No prior record of document being received in OEA.

Name:	Action:	Due Date:	Office:	Date Completed:	Initials:
[redacted]		06/05/2014	Administration & Operations Staff		

[redacted]

From: Michael Bardee
Sent: Thursday, May 29, 2014 8:09 AM
To: [redacted]
Cc: Edward Franks
Subject: Re: I/C (Rep. JeffDuncan) bulk power system security, Metcalf station (2014-00129)

[redacted]

On Thu, May 29, 2014 at 7:16 AM, [redacted] wrote:
> Mike/Ted: Please send me the names of the staff responsible for the
> actions below.
>
> Draft Response (OER) _____
>
> Review Draft Response (OER) _____
>
> Review Draft Response (OGC) _____
>
> Thanks!
>
> ---------- Forwarded message ----------
> From: [redacted]
> Date: Wed, May 28, 2014 at 5:30 PM
> Subject: I/C (Rep. JeffDuncan) bulk power system security, Metcalf
> station
> (2014-00129)
> To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring
> <Andrea.Spring@ferc.gov>, Andrew Weinstein
> <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>,
> David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber
> <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>,
> Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson
> <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray
> <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>,
> John Peschke <john.peschke@ferc.gov>, Kim Shannon
> <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura
> Vendetta <laura.vendetta@ferc.gov>, Leonard Tao
> <leonard.tao@ferc.gov>, Mary O'Driscoll <Mary.O'Driscoll@ferc.gov>,
> Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee
> <Michael.Bardee@ferc.gov>, Nicholas Tackett
> <nicholas.tackett@ferc.gov>, Patricia Herrion
> <Patricia.Herrion@ferc.gov>, Robert Ivanauskas
> <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin
> Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks
> <russell.fairbanks@ferc.gov>, Sandra Waldstein
> <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>,
> Shawn Bennett <Shawn.Bennett@ferc.gov>, Steven Wellner

> <steven.wellner@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
> Cc: [redacted] Craig Cano
> <craig.cano@ferc.gov>
>
>
>
> FOR YOUR INFORMATION ONLY.
>
> DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR
> BEFORE 06/05/14.
>
> --

[redacted]

>
>
>
> --

[redacted]

>
>
>
>

[redacted]

From: Michael Bardee
Sent: Tuesday, June 03, 2014 1:32 PM
To: J[redacted]
Cc: David Morenoff; Martin Kirkwood; [redacted]; Edward Franks; [redacted]
Subject: Re: I/C (Rep. JeffDuncan) bulk power system security, Metcalf station (2014-00129)

Ditto. Thanks, David.

On Tue, Jun 3, 2014 at 12:58 PM, [redacted] wrote:
> Looks fine here.
>
>
>
> From: David Morenoff [mailto:david.morenoff@ferc.gov]
> Sent: Tuesday, June 03, 2014 12:50 PM
> To: Michael Bardee
> Cc: Martin Kirkwood; [redacted] Edward
> Franks; [redacted]
> Subject: Re: I/C (Rep. JeffDuncan) bulk power system security, Metcalf
> station (2014-00129)
>
>
>
> Thanks, Mike. I marked a few suggested edits, [redacted]
> [redacted]s
> [redacted].
>
>
>
> David
>
>
>
> On Tue, Jun 3, 2014 at 11:55 AM, Michael Bardee
> <michael.bardee@ferc.gov>
> wrote:
>
> David/Martin/J[redacted] attached is a draft reply to controlled
> correspondence assigned to OER. If this looks okay to you, we will
> send it to you for signature etc.
>
> - Mike
>
>
> ---------- Forwarded message ----------
> From: [redacted]
> Date: Wed, May 28, 2014 at 5:30 PM
> Subject: I/C (Rep. JeffDuncan) bulk power system security, Metcalf

> station (2014-00129)
> To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring
> <Andrea.Spring@ferc.gov>, Andrew Weinstein
> <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>,
> David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber
> <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>,
> Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson
> <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray
> <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>,
> John Peschke <john.peschke@ferc.gov>, Kim Shannon
> <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura
> Vendetta <laura.vendetta@ferc.gov>, Leonard Tao
> <leonard.tao@ferc.gov>, Mary O'Driscoll <Mary.O'Driscoll@ferc.gov>,
> Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee
> <Michael.Bardee@ferc.gov>, Nicholas Tackett
> <nicholas.tackett@ferc.gov>, Patricia Herrion
> <Patricia.Herrion@ferc.gov>, Robert Ivanauskas
> <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin
> Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks
> <russell.fairbanks@ferc.gov>, Sandra Waldstein
> <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>,
> Shawn Bennett <Shawn.Bennett@ferc.gov>, Steven Wellner
> <steven.wellner@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
> Cc: [redacted] Craig Cano
> <craig.cano@ferc.gov>
>
>
>
> FOR YOUR INFORMATION ONLY.
>
> DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR
> BEFORE 06/05/14.
>
> --
[redacted]
>

[redacted]

From: Mark Hegerle
Sent: Tuesday, March 04, 2014 10:34 AM
To: Martin Kirkwood
Subject: Fwd: FW: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)
Attachments: 2014-00015.pdf; control sheet.pdf; 2014-00015-Cong Bridenstine (OK).docx

Per your request, here is the congressman's letter.

---------- Forwarded message ----------
From: **Mark Hegerle** <mark.hegerle@ferc.gov>
Date: Wed, Feb 26, 2014 at 12:06 PM
Subject: Fwd: FW: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)
To: Martin Kirkwood <martin.kirkwood@ferc.gov>
Cc: Edward Franks <Edward.Franks@ferc.gov>

Martin,

Attached is a proposed letter responding to a request by a congressman from Oklahoma concerning the Metcalf attack. The letter asks the following: *"I request an update on the FBI's investigation into this matter. I would also like your assessment regarding whether or not this attack qualifies as 'domestic terrorism.'"* [redacted]

Please review and comment this week, before I send it to Mike, as our draft letter is due to OE on Tuesday March 4.

Thanks,
Mark

---------- Forwarded message ----------
From: **Edward Franks** <edward.franks@ferc.gov>
Date: Tue, Feb 25, 2014 at 4:30 PM
Subject: FW: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)
To: mark.hegerle@ferc.gov

From: Michael Bardee [mailto:michael.bardee@ferc.gov]
Sent: Tuesday, February 25, 2014 1:50 PM
To: Edward Franks; [redacted]
Subject: Fwd: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)

Ted: have you seen this yet? We need to assign to someone, for quick turnaround.

- Mike

Sent from my iPad

Begin forwarded message:

From: [redacted]
Date: February 25, 2014 at 11:55:06 AM EST
To: "Aileen. Roder" <Aileen.Roder@ferc.gov>, Andrea Spring <Andrea.Spring@ferc.gov>, Andrew Weinstein <andrew.weinstein@ferc.gov>, chris murray <chris.murray@ferc.gov>, David Morenoff <david.morenoff@ferc.gov>, Felicia Abney-Barber <felicia.abney-barber@ferc.gov>, Jason Stanek <Jason.Stanek@ferc.gov>, Jeffery Dennis <Jeffery.Dennis@ferc.gov>, Jehmal Hudson <jehmal.hudson@ferc.gov>, Jennifer Quinlan Murray <Jennifer.Murray@ferc.gov>, Jette Gebhart <jette.gebhart@ferc.gov>, John Peschke <john.peschke@ferc.gov>, Joshua Konecni <Joshua.Konecni@ferc.gov>, Kim Shannon <Kim.Shannon@ferc.gov>, Kurt Longo <Kurt.Longo@ferc.gov>, Laura Vendetta <laura.vendetta@ferc.gov>, Leonard Tao <leonard.tao@ferc.gov>, "Mary O'Driscoll" <Mary.O'Driscoll@ferc.gov>, Meghan Estenson <meghan.estenson@ferc.gov>, Michael Bardee <Michael.Bardee@ferc.gov>, Nicholas Tackett <nicholas.tackett@ferc.gov>, Patricia Herrion <Patricia.Herrion@ferc.gov>, Robert Ivanauskas <Robert.Ivanauskas@ferc.gov>, Robin Lunt <robin.lunt@ferc.gov>, Robin Meidhof <robin.meidhof@ferc.gov>, Russell Fairbanks <russell.fairbanks@ferc.gov>, Sandra Waldstein <sandra.waldstein@ferc.gov>, Sarah McKinley <Sarah.McKinley@ferc.gov>, Shawn Bennett <Shawn.Bennett@ferc.gov>, Terence Burke <Terence.Burke@ferc.gov>
Cc: [redacted] Craig Cano <craig.cano@ferc.gov>
Subject: I/C (Rep. Bridenstine) bulk power system; security (2014-00015)

FOR YOUR INFORMATION ONLY.

DOCUMENT ASSIGNED TO OER FOR REPLY. DRAFT RESPONSE DUE TO OEA ON OR BEFORE 03/04/14.

[redacted]

JIM BRIDENSTINE
1ST DISTRICT, OKLAHOMA

216 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2211

2448 EAST 81ST STREET, SUITE 5150
TULSA, OKLAHOMA 74137
(918) 935-3222

Congress of the United States
House of Representatives
Washington, DC 20515-3601

COMMITTEE ON ARMED SERVICES

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY

Bridenstine.House.gov

Facebook.com/CongressmanJimBridenstine
Twitter.com/RepJBridenstine

February 12, 2014

Cheryl LaFleur
Acting Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Acting Commission LaFleur,

Like all Americans, my constituents in Oklahoma's First District rely on a safe and secure electric grid to function in our society. Therefore, I was troubled by a recent article in the *Wall Street Journal* (attached) describing an attack on a San Jose, California-based electrical substation. According to the *Journal*'s reporting, the Metcalf PG&E substation was attacked on April 16, 2013. The attackers subjected the Metcalf facility to a seemingly coordinated and sophisticated sniper attack. Indeed, the former Chairman of the Federal Energy Regulatory Commission (FERC), Jon Wellinghoff, described the attack as "domestic terrorism."

The Metcalf attack demonstrates the vulnerability of our electric grid, specifically its vital components that remain too easily exposed to physical attacks. As a Member of the House Armed Services Committee, I listed to frequent testimony from our military leadership regarding the consequences of cyberattack on this nation's critical infrastructure. The Metcalf shows that physical security is still very important even though cyber is much more in the news. I am concerned that the grid remains too vulnerable from a physical protection perspective.

According to the *Journal*, the FBI has made no arrests in the case. I request an update on the FBI's investigation into this matter. I would also like your assessment regarding whether or not this attack qualifies as "domestic terrorism". My staff member on this matter is James Mazol (james.mazol@mail.house.gov).

Sincerely,

Jim Bridenstine

2014-00015

Assault on California Power Station Raises Alarm on Potential for Terrorism

April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid

Feb. 4, 2014 10:30 p.m. ET

SAN JOSE, Calif.—The attack began just before 1 a.m. on April 16 last year, when someone slipped into an underground vault not far from a busy freeway and cut telephone cables.

Within half an hour, snipers opened fire on a nearby electrical substation. Shooting for 19 minutes, they surgically knocked out 17 giant transformers that funnel power to Silicon Valley. A minute before a police car arrived, the shooters disappeared into the night.

A sniper attack in April that knocked out an electrical substation near San Jose, Calif., has raised fears that the country's power grid is vulnerable to terrorism. WSJ's Rebecca Smith has the details. Photo: Talia Herman for The Wall Street Journal

With over 160,000 miles of transmission lines, the U.S. power grid is designed to handle natural and man-made disasters, as well as fluctuations in demand. How does the system work? WSJ's Jason Bellini has #TheShortAnswer.

To avoid a blackout, electric-grid officials rerouted power around the site and asked power plants in Silicon Valley to produce more electricity. But it took utility workers 27 days to make repairs and bring the substation back to life.

Nobody has been arrested or charged in the attack at PG&E Corp.'s PCG +0.09% PG&E Corp. U.S.: NYSE $42.48 +0.04 +0.09% Feb. 12, 2014 9:40 am Volume (Delayed 15m) : 0 P/E Ratio 26.21 Market Cap $19.07 Billion Dividend Yield 4.29% Rev. per Employee $757,442 02/11/14 PG&E swings to profit with few... 02/09/14 U.S. Utilities Tighten Securit... 02/05/14 Q&A: What You Need to Know Abo... More quote details and news » PCG in Your Value Your Change Short position Metcalf transmission substation. It is an incident of which few Americans are aware. But one former federal regulator is calling it a terrorist act that, if it were widely replicated across the country, could take down the U.S. electric grid and black out much of the country.

The attack was "the most significant incident of domestic terrorism involving the grid that has ever occurred" in the U.S., said Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time.

The Wall Street Journal assembled a chronology of the Metcalf attack from filings PG&E made to state and federal regulators; from other documents including a video released by the Santa Clara County Sheriff's Department; and from interviews, including with Mr. Wellinghoff.

Related

Q&A: What You Need to Know About Attacks on the U.S. Power Grid

The 64-year-old Nevadan, who was appointed to FERC in 2006 by President George W. Bush and stepped down in November, said he gave closed-door, high-level briefings to federal agencies, Congress and the White House last year. As months have passed without arrests, he said, he has grown increasingly concerned that an even larger attack could be in the works. He said he was going public about the incident out of concern that national security is at risk and critical electric-grid sites aren't adequately protected.

The Federal Bureau of Investigation doesn't think a terrorist organization caused the Metcalf attack, said a spokesman for the FBI in San Francisco. Investigators are "continuing to sift through the evidence," he said.

Some people in the utility industry share Mr. Wellinghoff's concerns, including a former official at PG&E, Metcalf's owner, who told an industry gathering in November he feared the incident could have been a dress rehearsal for a larger event.

"This wasn't an incident where Billy-Bob and Joe decided, after a few brewskis, to come in and shoot up a substation," Mark Johnson, retired vice president of transmission for PG&E, told the utility security conference, according to a video of his presentation. "This was an event that was well thought out, well planned and they targeted certain components." When reached, Mr. Johnson declined to comment further.

A spokesman for PG&E said the company takes all incidents seriously but declined to discuss the Metcalf event in detail for fear of giving information to potential copycats. "We won't speculate about the motives" of the attackers, added the spokesman, Brian Swanson. He said PG&E has increased security measures.

Utility executives and federal energy officials have long worried that the electric grid is vulnerable to sabotage. That is in part because the grid, which is really three systems serving different areas of the U.S., has failed when small problems such as trees hitting transmission lines created cascading blackouts. One in 2003 knocked out power to 50 million people in the Eastern U.S. and Canada for days.

Many of the system's most important components sit out in the open, often in remote locations, protected by little more than cameras and chain-link fences.

Transmission substations are critical links in the grid. They make it possible for electricity to move long distances, and serve as hubs for intersecting power lines.

Within a substation, transformers raise the voltage of electricity so it can travel hundreds of miles on high-voltage lines, or reduce voltages when electricity approaches its destination. The Metcalf substation functions as an off-ramp from power lines for electricity heading to homes and businesses in Silicon Valley.

The country's roughly 2,000 very large transformers are expensive to build, often costing millions of dollars each, and hard to replace. Each is custom made and weighs up to 500,000 pounds, and "I can only build 10 units a month," said Dennis Blake, general manager of Pennsylvania Transformer in Pittsburgh, one of seven U.S. manufacturers. The utility industry keeps some spares on hand.

A 2009 Energy Department report said that "physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale...could result in prolonged outages, as procurement cycles for these components range from months to years."

Mr. Wellinghoff said a FERC analysis found that if a surprisingly small number of U.S. substations were knocked out at once, that could destabilize the system enough to cause a blackout that could encompass most of the U.S.

Not everyone is so pessimistic. Gerry Cauley, chief executive of the North America Electric Reliability Corp., a standards-setting group that reports to FERC, said he thinks the grid is more resilient than Mr. Wellinghoff fears.

"I don't want to downplay the scenario he describes," Mr. Cauley said. "I'll agree it's possible from a technical assessment." But he said that even if several substations went down, the vast majority of people would have their power back in a few hours.

The utility industry has been focused on Internet attacks, worrying that hackers could take down the grid by disabling communications and important pieces of equipment. Companies have reported 13 cyber incidents in the past three years, according to a Wall Street Journal analysis of emergency reports utilities file with the federal government. There have been no reports of major outages linked to these events, although companies have generally declined to provide details.

"A lot of people in the electric industry have been distracted by cybersecurity threats," said Stephen Berberich, chief executive of the California Independent System Operator, which runs much of the high-voltage transmission system for the utilities. He said that physical attacks pose a "big, if not bigger" menace.

There were 274 significant instances of vandalism or deliberate damage in the three years, and more than 700 weather-related problems, according to the Journal's analysis.

Until the Metcalf incident, attacks on U.S. utility equipment were mostly linked to metal thieves, disgruntled employees or bored hunters, who sometimes took potshots at small transformers on utility poles to see what happens. (Answer: a small explosion followed by an outage.)

Last year, an Arkansas man was charged with multiple attacks on the power grid, including setting fire to a switching station. He has pleaded not guilty and is undergoing a psychiatric evaluation, according to federal court records.

Overseas, terrorist organizations were linked to 2,500 attacks on transmission lines or towers and at least 500 on substations from 1996 to 2006, according to a January report from the Electric Power Research Institute, an industry-funded research group, which cited State Department data.

An attack on a PG&E substation near San Jose, Calif., in April knocked out 17 transformers like this one. Talia Herman for The Wall Street Journal

To some, the Metcalf incident has lifted the discussion of serious U.S. grid attacks beyond the theoretical. "The breadth and depth of the attack was unprecedented" in the U.S., said Rich Lordan, senior technical executive for the Electric Power Research Institute. The motivation, he said, "appears to be preparation for an act of war."

The attack lasted slightly less than an hour, according to the chronology assembled by the Journal.

At 12:58 a.m., AT&T fiber-optic telecommunications cables were cut—in a way that made them hard to repair—in an underground vault near the substation, not far from U.S. Highway 101 just outside south San Jose. It would have taken more than one person to lift the metal vault cover, said people who visited the site.

Nine minutes later, some customers of Level 3 Communications, LVLT +0.35% Level 3 Communications Inc. U.S.: NYSE $36.83 +0.13 +0.35% Feb. 12, 2014 9:39 am Volume (Delayed 15m) : 0 P/E Ratio N/A Market Cap $8.21 Billion Dividend Yield N/A Rev. per Employee $584,537 02/05/14 Level 3 Swings to Profit on Lo... 01/27/14 Puzzle for CFOs: Fixed or Floa... 11/26/13 The Morning Download: NSA Reve... More quote details and news » LVLT in Your Value Your Change Short position an Internet service provider, lost service. Cables in its vault near the Metcalf substation were also cut.

At 1:31 a.m., a surveillance camera pointed along a chain-link fence around the substation recorded a streak of light that investigators from the Santa Clara County Sheriff's office think was a signal from a waved flashlight. It was followed by the muzzle flash of rifles and sparks from bullets hitting the fence.

The substation's cameras weren't aimed outside its perimeter, where the attackers were. They shooters appear to have aimed at the transformers' oil-filled cooling systems. These began to bleed oil, but didn't explode, as the transformers probably would have done if hit in other areas.

About six minutes after the shooting started, PG&E confirms, it got an alarm from motion sensors at the substation, possibly from bullets grazing the fence, which is shown on video.

Four minutes later, at 1:41 a.m., the sheriff's department received a 911 call about gunfire, sent by an engineer at a nearby power plant that still had phone service.

Riddled with bullet holes, the transformers leaked 52,000 gallons of oil, then overheated. The first bank of them crashed at 1:45 a.m., at which time PG&E's control center about 90 miles north received an equipment-failure alarm.

Five minutes later, another apparent flashlight signal, caught on film, marked the end of the attack. More than 100 shell casings of the sort ejected by AK-47s were later found at the site.

At 1:51 a.m., law-enforcement officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.

A PG&E worker, awakened by the utility's control center at 2:03 a.m., arrived at 3:15 a.m. to survey the damage.

Grid officials routed some power around the substation to keep the system stable and asked customers in Silicon Valley to conserve electricity.

In a news release, PG&E said the substation had been hit by vandals. It has since confirmed 17 transformers were knocked out.

Mr. Wellinghoff, then chairman of FERC, said that after he heard about the scope of the attack, he flew to California, bringing with him experts from the U.S. Navy's Dahlgren Surface Warfare Center in Virginia, which trains Navy SEALs. After walking the site with PG&E officials and FBI agents, Mr. Wellinghoff said, the military experts told him it looked like a professional job.

In addition to fingerprint-free shell casings, they pointed out small piles of rocks, which they said could have been left by an advance scout to tell the attackers where to get the best shots.

"They said it was a targeting package just like they would put together for an attack," Mr. Wellinghoff said.

Mr. Wellinghoff, now a law partner at Stoel Rives LLP in San Francisco, said he arranged a series of meetings in the following weeks to let other federal agencies, including the Department of Homeland Security, know what happened and to enlist their help. He held a closed-door meeting with utility executives in San Francisco in June and has distributed lists of things utilities should do to strengthen their defenses.

A spokesman for Homeland Security said it is up to utilities to protect the grid. The department's role in an emergency is to connect federal agencies and local police and facilitate information sharing, the spokesman said.

As word of the attack spread through the utility industry, some companies moved swiftly to review their security efforts. "We're looking at things differently now," said Michelle Campanella, an FBI veteran who is director of security for Consolidated Edison Inc. ED -0.99% Consolidated Edison Inc. U.S.: NYSE $53.89 -0.54 -0.99% Feb. 12, 2014 9:40 am Volume (Delayed 15m) : 0 P/E Ratio 15.38 Market Cap $15.94 Billion Dividend Yield 4.63% Rev. per Employee $852,158 01/14/14 Con Ed Rates, Frozen For Now, ... More quote details and news » ED in Your Value Your Change Short position in New York. For example, she said, Con Ed changed the angles of some of its 1,200 security cameras "so we don't have any blind spots."

Some of the legislators Mr. Wellinghoff briefed are calling for action. Rep. Henry Waxman (D., Calif.) mentioned the incident at a FERC oversight hearing in December, saying he was concerned that no one in government can order utilities to improve grid protections or to take charge in an emergency.

As for Mr. Wellinghoff, he said he has made something of a hobby of visiting big substations to look over defenses and see whether he is questioned by security details or local police. He said he typically finds easy access to fence lines that are often close to important equipment.

"What keeps me awake at night is a physical attack that could take down the grid," he said. "This is a huge problem."

—Tom McGinty contributed to this article.

Write to Rebecca Smith at rebecca.smith@wsj.com

Federal Energy Regulatory Commission
Correspondence Control Sheet Report
(Sorted by Document Number)

Document No: 2014-00015

	Priority:	Regular	Via:	Mail	Date of Document : 02/12/2014
Signature: LaFleur, Cheryl	Type :	Electric	Form :	Letter	Date Received : 02/25/2014
	Reply :	Yes	Origin :	Incoming	Date Due : 03/11/2014

Authors Name	Company & Title		
Bridenstine, Jim	Congressman	US House	OK

Subject : bulk power system; security

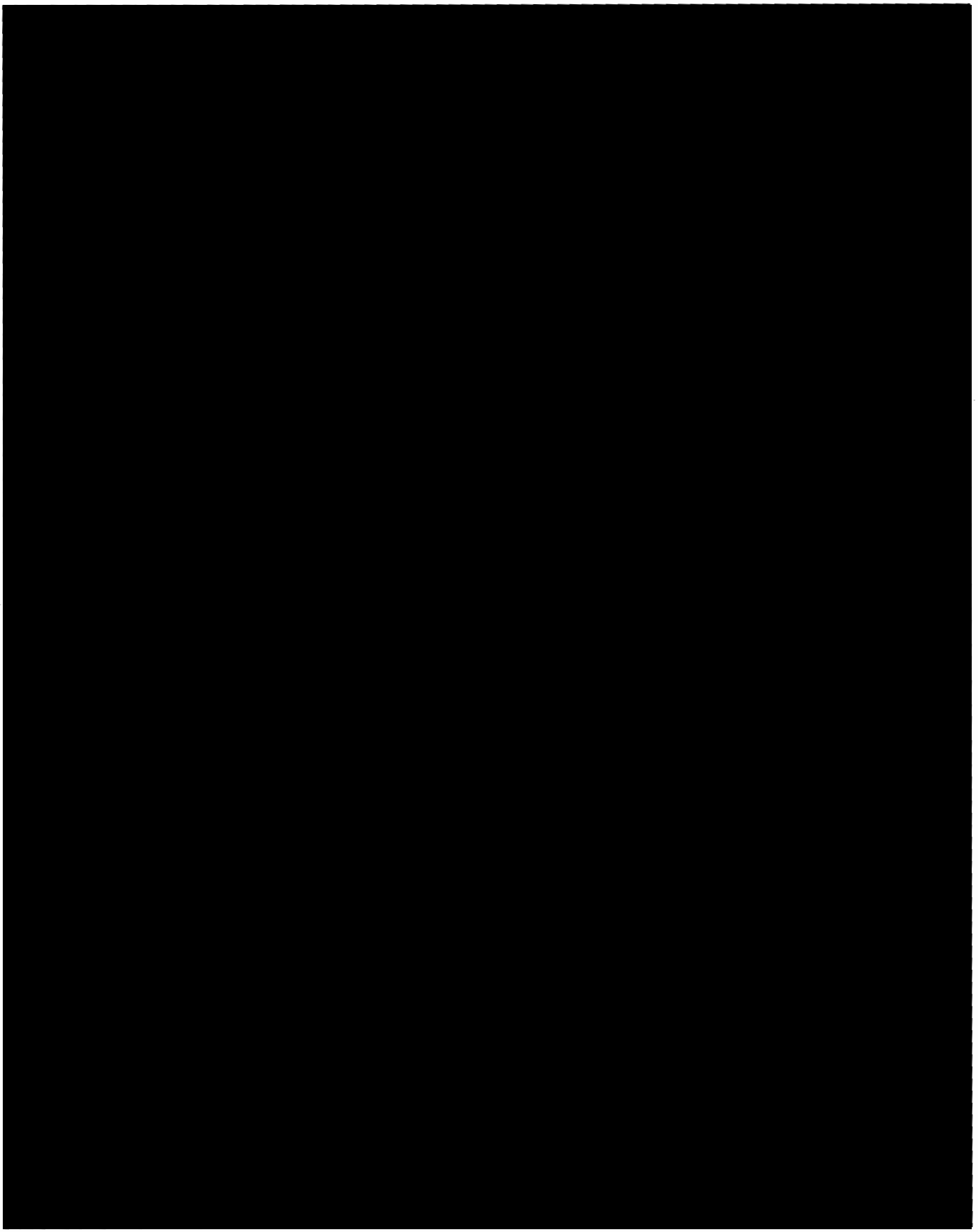
Dockets :

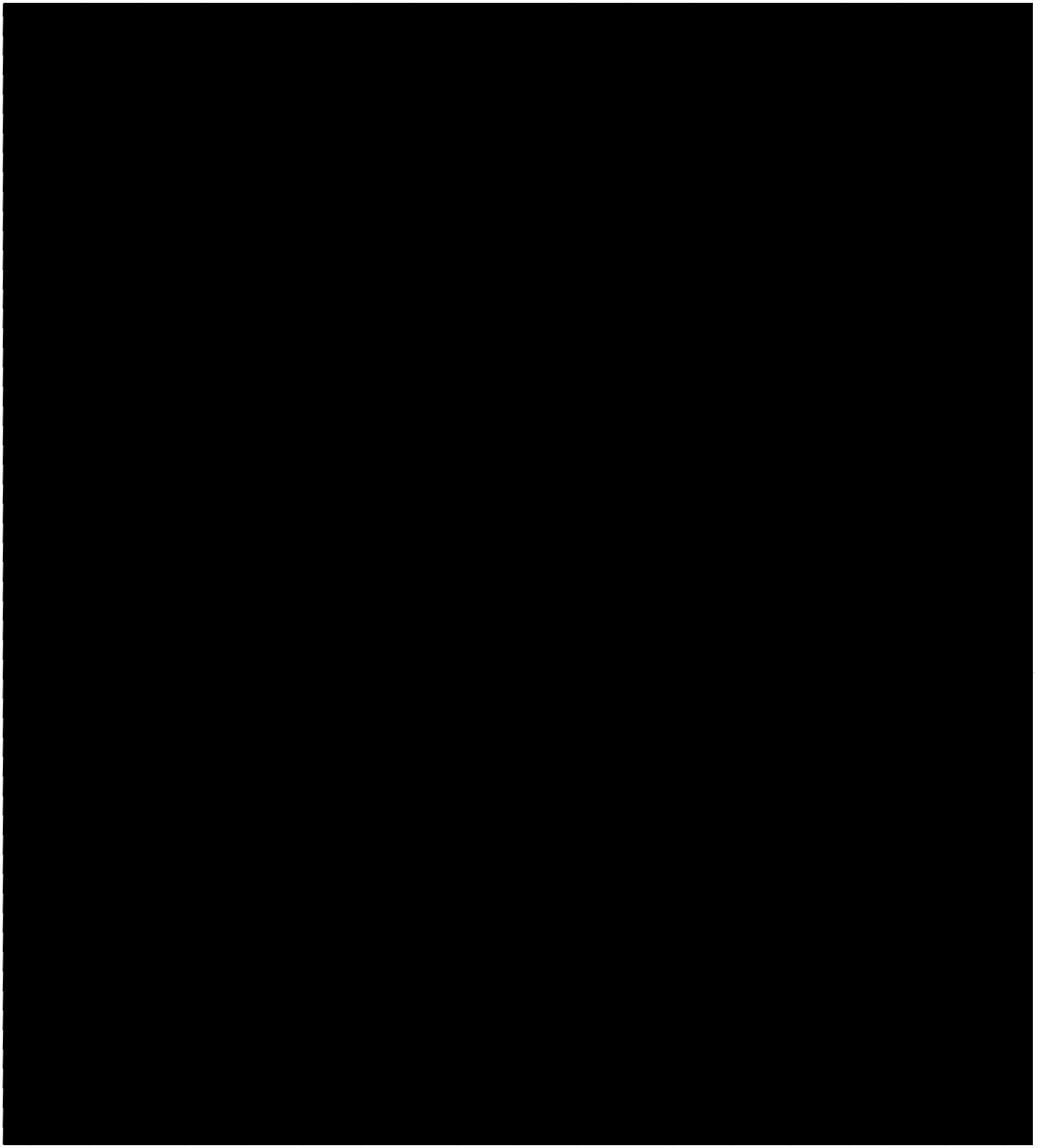
Class : Congressional

Infocopy : Moeller Norris LaFleur Clark

Notes: No applicable notes.

Name:	Action:	Due Date:	Office:	Date Completed:	Initials:
[redacted]	Assignment	03/04/2014	Administration & Operations Staff		





From: [redacted]
Sent: Monday, June 03, 2013 7:33 AM
To: [redacted] Edward Franks; [redacted]; Cynthia Pointer; [redacted] Joseph McClelland; [redacted]
Subject: Fwd: Current Situation Report, 5/31
Attachments: 05-31-2013 Current Situation Report.pdf

Greetings,

Attached is last week's Current Situation Report, including the following articles:

- ICS-CERT Issues Advisory for Vulnerability in the 3S CODESYS Gateway Application

- Lofty Perch President Mark Fabro Discusses Importance of Developing a Security Culture

- Department of Justice Deputy Attorney General James Cole Suggests Cybersecurity Practices

- FERC Chairman Jon Wellinghoff Announces Resignation

- Electric Power Research Institute's Annabelle Lee on Cryptographic Key Management

- Bipartisan Commission Releases Report on Impacts of International Intellectual Property Theft

- The Basics of Quantum Cryptography Discussed in *The Economist*

Best regards,

[redacted]

Current Situation: Energy Delivery Systems Security

Prepared by Energetics Incorporated for the National SCADA Test Bed Program (NSTB)

May 31, 2013

Vulnerabilities and Cyber Incidents

- **ICS-CERT Issues Advisory for Vulnerability in the 3S CODESYS Gateway Application,** http://ics-cert.us-cert.gov/advisories/ICSA-13-142-01. A denial-of-service vulnerability was identified by independent researcher Nicholas Miles, which may allow an attacker to remotely crash the Gateway server application or execute arbitrary code if exploited. 3S has developed an update to mitigate the vulnerability.

Events and Interviews

- **Lofty Perch President Mark Fabro Discusses Importance of Developing a Security Culture,** http://www.theregister.co.uk/2013/05/23/scada_security/. Speaking at AusCERT 2013, Fabro discussed how SCADA operators play a role in defending against attackers because they can notice unusual processes that occur and take some sort of action. At the same time, personnel can be the tipping point for an intrusion, where an individual may perform an inappropriate action such as inadvertently clicking on a malicious link.
- **Department of Justice Deputy Attorney General James Cole Suggests Cybersecurity Practices,** http://www.networkworld.com/community/node/83098. Speaking at the Georgetown Cybersecurity Law Institute, Cole said that companies and the government can work together to combat cyber threats through prevention, preparedness, and incident response. He discussed other areas that companies should consider, including education, information sharing, and financial obligation to stakeholders.

Federal Agency Cybersecurity Programs and Hearings

- **FERC Chairman Jon Wellinghoff Announces Resignation,** http://www.powermag.com/POWERnews/FERC-Chair-Wellinghoff-Announces-Resignation_5674.html. Wellinghoff's term ends June 30, and is expected to remain as chair at least until a replacement has been confirmed by the Senate. Wellinghoff was appointed as commissioner in 2006 and named chairman in 2009. During his tenure, FERC implemented changes to confront cyber attacks and boost infrastructure investment.

Reports and Surveys

- **Electric Power Research Institute's Annabelle Lee on Cryptographic Key Management,** http://online.electricity-today.com/doc/electricity-today/et_may_2013_digital/2013051701/#42. The May issue *of Electricity Today Magazine* includes an article by Lee, which provides an overview of the variety of data protections that cryptography can provide, along with considerations for applying cryptographic key management systems to advanced metering infrastructure.
- **Bipartisan Commission Releases Report on Impacts of International Intellectual Property Theft,** http://www.forbes.com/sites/emmawoollacott/2013/05/23/us-should-get-tough-on-chinese-ip-theft-committee-warns/. Developed by the Commission on the Theft of American Intellectual Property, the report discusses how cyber espionage is a growing problem and how long supply chains present a challenge to identifying exploited technologies. The report provides over 20 short, mid, and long term

recommendations to mitigate IP theft. *The IP Commission Report* can be found here: http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Other Related-Cyber Issues

- **The Basics of Quantum Cryptography Discussed in *The Economist*,** http://www.economist.com/news/science-and-technology/21578358-eavesdropping-secret-communications-about-get-harder-solace. The article provides an overview of quantum cryptography methods as well as various activities underway, including the pocket-sized QKD transmitter being developed by Los Alamos National Laboratory.

No Relevant News Items for These Categories:

- Standards and Policies
- Cyberwar and Cyberterrorism
- Training, Education, and Collaboration

[redacted]

From: CI Reports <reports@critical-intelligence.com>
Sent: Friday, February 14, 2014 12:25 PM
Subject: [ICS SECURITY ARTICLE DIGEST]

[redacted]

4/13: San Jose Substation Attack 5/13: Wellinghoff announces FERC resignation (joins Stoel Rives) [redacted]

[redacted]

Non-Responsive [redacted]

From: Sarah McKinley
Sent: Friday, May 31, 2013 3:41 PM
To: [redacted]
Subject: Communication Chronicle (May 31, 2013)
Attachments: Communication Chronicle - 5 31-2013.docx

The Communication Chronicle Vol. 203

[redacted]

[redacted]

[redacted]

• **Media Calls** – This week reporters called about: Chairman Wellinghoff's resignation announcement [redacted]

[redacted]

From: David Andrejcak
Sent: Thursday, June 06, 2013 10:03 AM
To: Joseph McClelland
Subject: RE: June 3 newsclips

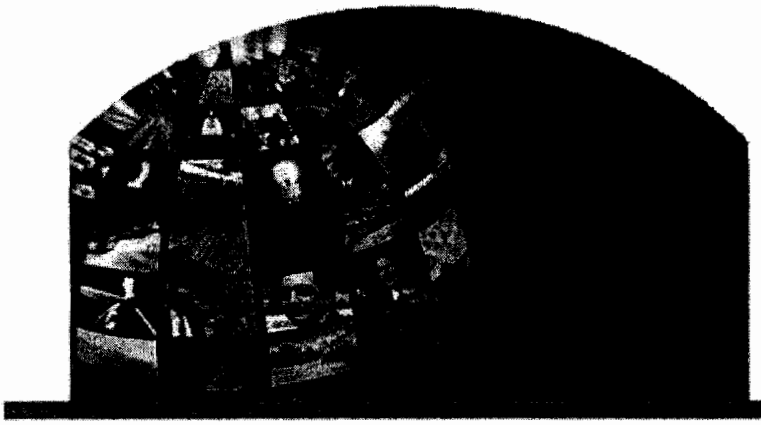
[redacted]

From: Joseph McClelland [mailto:joseph.mcclelland@ferc.gov]
Sent: Thursday, June 06, 2013 9:56 AM
To: David Andrejcak
Subject: Fwd: June 3 newsclips
Third article.

Sent from my iPad

Begin forwarded message:

> **From:** Media DL <mediadl@ferc.gov>
> **Date:** June 3, 2013, 8:40:30 AM EDT
> **To:** NewsDL <newsdl@ferc.gov>
> **Subject: June 3 newsclips**



DAILY
NEWS C
OFFICE OF EXTERNAL .
FEDERAL ENERGY REGULATOR
Contact mediadl@fer

Monday, June 3, 2013 Visit our News Clips website

TOP STORIES. 2

7217

Top Stories

SNL.com
Friday, May 31, 2013 6:08 PM ET

Praised as a tough 'cop on the beat,' FERC's Wellinghoff says manipulators must feel pain

By Glen Boshart

During a May 31 interview on C-SPAN, departing Federal Energy Regulatory Commission Chairman Jon Wellinghoff received high praise from several callers for his stern demeanor and appearance as a tough "cop on the beat" who is looking out for potential manipulation of wholesale power and natural gas markets.

The show's host also pointed to a recent article in The Baltimore Sun praising Wellinghoff for his "aggressive approach" in taking on Wall Street banks and large energy firms, especially in comparison to other regulators charged with looking for manipulation in the oil and gasoline

markets. Sen. Maria Cantwell, D-Wash., has also praised Wellinghoff for his tough stance on market manipulation.

"Just seeing your appearance, you seem like a pretty serious guy," said one caller from eastern Connecticut. "You look like a tough guy who gets the job done." The caller went on to say that if the people in charge of the agencies tasked with overseeing the banking and other industries that "perpetuate scams" were more like Wellinghoff, "the country would be a lot better off."

Wellinghoff, who recently announced that he plans to step away from FERC after almost seven years as a commissioner, attributed his agency's aggressive approach to tracking down energy market manipulators under his watch to the passage of energy legislation in 2005 and the extra resources he has dedicated to that effort since he became chairman more than four years ago.

The Energy Policy Act of 2005 boosted FERC's market oversight authorities and raised the amount the agency could penalize a company that engages in market manipulation from just $10,000 per day of illegal activity to $1 million per day, Wellinghoff explained. He also recalled that FERC had less than 10 employees assigned to ferreting out market manipulation when Enron's downfall occurred in late 2001, while it now has more than 200 people analyzing data and looking for suspicious market behavior and anomalies.

Wellinghoff suggested that his agency has not been shy in pursuing large penalties when it does discover market manipulation — a unit of Constellation Energy Group Inc. agreed to pay a $135 million fine in March 2012, and FERC is considering a recommendation by its staff that Barclays Bank PLC be forced to pay a record $469.9 million penalty — because sanctions have to send the proper message.

"If you go into a market and take $100 million out of it improperly, then the fine needs to be some multiple of that so that they know it's not just a traffic ticket; it's not just something that they can write off on their bottom line and do again and not fear the economic consequences," Wellinghoff stated.

As for how high the financial consequences will have to be to hurt JPMorgan Chase & Co. if FERC decides to pursue penalties in its investigation of that company's activities, Wellinghoff refused to speculate since that case is still ongoing. However, he said any penalties imposed by the agency for market manipulation have "to hurt enough so they don't do it again" and so other companies are deterred from engaging in similar activity.

Asked why he has decided not to seek another term once his current term expires June 30, he said that the time has simply come for him to move on after being with the agency for almost seven years and serving as its chairman for more than four. He insisted that he "has done a lot" during that time, citing a number of wide-ranging new rules and initiatives designed to encourage broader regional planning, energy efficiency and demand response. It simply is time to turn the reins of FERC over "to a new class," he maintained.

Wellinghoff has said he plans to stay on at the agency until the next head of FERC has been nominated or confirmed. If no one is established as his replacement in the meantime, he could stay on in that role until the end of the current congressional session.

While a number of people have been rumored to be in the running as Wellinghoff's potential replacement, including current FERC Commissioners John Norris and Cheryl LaFleur, the manner of Wellinghoff's resignation appears to indicate that the next chairman may come from outside the agency.

Gossip among Washington insiders suggests that the president may select Rose McKinney-James, who has ties to the Obama administration and is rumored to have the support of Senate Majority Leader Harry Reid. McKinney-James is the managing principal of Energy Works Consulting and of McKinney-James & Associates, both of which are based in Las Vegas.

Return to Top
Greenwire

FERC: Outgoing chairman fields calls on C-SPAN, reflects on his legacy

Hannah Northey, E&E reporter

Published: Friday, May 31, 2013

The chairman of the Federal Energy Regulatory Commission said today that he's stepping down because he has been there "a long time" and has managed to push through major reforms in grid planning and oversight of the energy markets.

"I've been there seven years, which is a long time for a FERC commissioner," Chairman Jon Wellinghoff said during an interview with C-SPAN's "Washington Journal." "I think it's time to move on, look for other opportunities and sort of turn it over to the next group."

Wellinghoff came to FERC to fill a vacant seat in 2006 and was reconfirmed in 2008 for a full five-year term as a commissioner. President Obama tapped him in March 2009 to become chairman; his current term expires at the end of next month.

During his tenure, the former Nevada consumer advocate ushered in far-reaching rules to revamp how new power lines are planned and paid for, and eased the path for renewable generators to connect to the grid. He also oversaw the agency's implementation of new policies to strengthen demand response and spark innovative transmission and "smart grid" technologies.

"I've done a lot there, and I think it's time to turn it over to a new class," he said.

Wellinghoff will continue leading the commission and its 1,500 employees until Obama picks a replacement and secures Senate confirmation.

There is a lot of talk in Washington about whom the president might choose. Sources have pointed to FERC's two sitting Democratic commissioners, Cheryl LaFleur and John Norris (Greenwire, May 29).

Wellinghoff said little about what's next for him, but he vowed to recuse himself from any votes involving firms he'll be speaking with in coming months. Federal rules will prohibit him from doing business before the commission for one year after his departure.

He touched on the agency's stepped-up oversight of manipulation in the wholesale power and gas markets, and said FERC has already collected enough in fees from users and fines from manipulation cases to cover its annual budget of more than $300 million.

"We already almost paid for ourselves," he said.

FERC has recently stepped up its oversight of market manipulation and collected millions in fines from Wall Street banks accused of gaming power markets, including Constellation Energy Commodities Group. Wellinghoff said scrutiny has ramped up since the 2001 Enron scandal and since FERC obtained more authority under federal law to oversee the markets and impose fines of up to $1 million daily.

"I think we're actually doing it very effectively in the sense that I think we're corralling in the good portion of what fraud there is out there," he said. "We're seeing a lot less now, certainly, than we did see back in the Enron days, so I think we can have confidence in these markets going forward."

The chairman did not provide a timeline for when FERC would conclude its investigation of JPMorgan Chase & Co. FERC has accused the bank of overcharging grid operators and customers in Michigan and California up to $83 million, drawing the ire of lawmakers from

those states (Greenwire, May 30). The timeline could depend on whether FERC settles the case or issues an order, he said.

The outgoing chairman also took questions from C-SPAN callers, some angry over the agency's approval of new gas pipelines to ship around a newfound glut of shale gas.

"I got breast cancer because of you, buddy," said one caller who said she got sick from methane leaking into a nearby well.

Wellinghoff said that such issues are not under FERC's jurisdiction and instead are handled by the federal or state environmental agencies, and that he does believe gas can be developed responsibly.

"We have to recognize there are trade-offs we have to make to ensure we can have the quality of life" we desire, he said. "That doesn't mean it can't be done in an environmentally sensitive way to minimize damage" to consumers and the environment.

Wellinghoff also said he believes that potential exports of domestic natural gas will not cause prices to spike, noting that export terminals -- that FERC must approve -- are expensive and time-consuming to build. Instead, the United States is likely to see production continue to increase and new shale plays will be found, and prices will remain relatively stable, he said.

"We're seeing new availabilities of gas that we never even knew were in existence," he said. "The price is going to stay very stable for a long time, between the $3 and $6 range."

Return to Top

Inside FERC

June 3, 2013

Wellinghoff set to resign once replacement is confirmed, will continue to lead commission and vote

Chairman Jon Wellinghoff has told President Obama that he will step down from FERC once a replacement is confirmed by the Senate, a commission official said last week, confirming rumors that had swirled through the Washington energy community over the past few weeks.

In the meantime, Wellinghoff "will continue as chairman and vote on matters before the commission," said FERC spokesman Craig Cano.

The commission's 12th chairman, Wellinghoff has headed FERC since January 2009 and presided over major rulemakings on transmission planning and cost allocation, renewable energy, conservation and demand response. His extensive legacy also includes aggressive monitoring and investigation of energy market manipulation and restructuring of the commission's offices to emphasize infrastructure protection and policy and innovation.

Wellinghoff's current term expires at the end of June, after which he can continue to serve during a grace period running through the current session of Congress.

Sources told Platts earlier last week that Wellinghoff had told senior staff of his plans and that a public announcement would be made soon.

Attention now turns to Wellinghoff's replacement, and various sources have said the new commissioner likely will be named chairman. According to one source, an announcement from the White House on the nominee is imminent.

Candidates said to be in the running for the spot include: Rose McKinney-James, a former Nevada Public Service Commission member with ties to the Obama presidential campaign and Senate Majority Leader Harry Reid; Ron Binz, a former chairman of the Colorado Public

Utilities Commission; Collette Honorable, chairman of the Arkansas Public Service Commission; and attorney Regina Speed-Bost, a partner with Schiff Hardin.

Speed-Bost, who started her career at FERC, said it "would be an honor to serve on the commission," though she added that there had been no official conversations with the White House. "I believe I know the industry very well, and would have something to offer" if chosen, she said.

A call to McKinney-James seeking comment was not returned by press time. Honorable and Binz declined to comment.

While serving as chairman of the Colorado PUC from January 2007 to April 2011, Binz was an active member of the National Association of Regulatory Utility Commissioners. Prior to that, he was an energy and telecommunications consultant, served as president of the Competition Policy Institute and directed the Colorado Office of Consumer Counsel.

Honorable's name has come up before, and she would provide Southern state representation currently lacking at the commission. She has served on the Arkansas commission since 2007 and was named chairman in January 2011.

Senator Ron Wyden, chairman of the Energy and Natural Resources Committee, was among those who touted Wellinghoff's accomplishments at FERC. "Under Chairman Wellinghoff's leadership, FERC launched important investigations to protect consumers against traders and financial firms who manipulated energy markets," said the Oregon Democrat. "While we disagreed on electric transmission siting issues, he deserves credit for championing efforts to increase America's renewable energy supply."

NARUC President Philip Jones applauded Wellinghoff's efforts to "help build understanding and bridge differences" between federal and state regulators. "Although we have had our disagreements . . . we utilized our collaborative dialogues to maintain a positive relationship."

Wellinghoff's strong support for development of demand response resources was reflected in remarks by Dan Delurey, executive director of the Association for Demand Response and Smart Grid.

The chairman "moved the demand response ball down the court, beyond just 'curtailment' programs aimed at ensuring reliability," said Delurey, adding that Wellinghoff's "vision and forethought . . . puts him among a rare group of policymakers who can be said to have helped an entire industry turn a corner and move in a new direction."

With backing in the Senate by Reid, Wellinghoff was confirmed and joined FERC in 2006 as a commissioner. In a December 2007 package deal involving a new term for then-Chairman Joseph Kelliher, Wellinghoff received a fresh five-year term.

Following his first inauguration in January 2009, Obama elevated Wellinghoff to chairman, replacing Kelliher.

Before joining FERC, Wellinghoff was in private law practice. He also served two terms as Nevada's first consumer advocate. In that role, he represented utility consumers before the Public Utilities Commission of Nevada, FERC and in appeals before the Nevada Supreme Court.

Chris Newkumet

Return to Top

Electricity Policy

Jon Wellinghoff's legacy at FERC? Judgment must wait on future results

By Kennedy Maize

May 31, 2013 – Jon Wellinghoff is leaving the Federal Energy Regulatory Commission sometime soon. What legacy does he leave behind? It's a difficult question to answer, in part because of what he brought to the commission to begin with.

While a lawyer, like most FERC commissioners, Wellinghoff was different than most prior commissioners in that he was neither a Washington insider nor a former state utility regulator. He was a state consumer advocate, the first ever to get a slot at FERC, and coming from an institutional environment skeptical of how regulators have operated. He was truly an outsider.

Here are some of the most memorable past FERC appointees,: Charlie Curtis (former House staffer), Rick Richard (former Senate staffer), Chuck Trabandt (former Senate staffer), Betsy Moler (former Senate staffer), Branko Terzic (former state regulator), Curt Hebert (former state regulator), Mark Spitzer (former state regulator), John Norris (former state regulator), Tony Clark (former state regulator).

Unlike most of his predecessors, Wellinghoff spent much of his earlier career challenging state regulators and federal laws and rules from the outside. Before his FERC appointment, Wellinghoff served two terms as Nevada's first utility consumer advocate. As he proudly noteson his section of the FERC web site, in Nevada he wrote the first state integrated planning law for utilities and was the "primary author" of the state's renewable energy portfolio standard.

Wellinghoff was never particularly close to state regulators and at FERC had frequent polite disagreements with the National Association of Regulatory Utility Commissioners. Upon his resignation announcement, Washington state regulator Philip Jones, the current president of NARUC, said, "Under his watch, Chair Wellinghoff spearheaded the several FERC-NARUC collaborative dialogues on issues of regional and national concern. These discussions help build understanding and bridge differences between federal and State regulators. Although we have had our disagreements, as there is always a natural tension between State and federal governments, we utilized our collaborative dialogues to maintain a positive relationship."

When Wellinghoff was first named to the commission in 2006 as a minority member, at the behest of Senate Majority Leader Harry Reid (D-Nev.), he scarcely made a ripple and drew no notice even from the New York Times. When named chairman in 2009, the Times highlighted his green credentials, quoting the veteran Natural Resources Defense Council electricity guru Ralph Cavanagh, "He's been a consistent advocate of sustainable energy policies — energy efficiency, renewable energy and clean distributed resources, and he has focused on making sure these resources are treated fairly in energy markets (many of which had been notorious for hostility to these relative newcomers)."

What stands as Wellinghoff's signature accomplishments as a federal regulator? Several accounts properly point to FERC's Order No. 1000, which he championed and pushed through the commission approval process.

This is the FERC rule that dramatically changes the way the transmission grid will be planned and developed in the future, mandating a collaborative regional process. The order has drawn fire from the two Republicans on the commission for its provision that drops FERC's prior deference to incumbent transmission owners, as well as the commission's willingness to ignore the historic preference for honoring existing contracts, blessed by the Supreme Court as the Mobile Sierra doctrine.

The implementation of Order No. 1000 has been slower and more contentious than Wellinghoff and the commission majority intended. But it has gone forward. Whether future commissions will continue the emphasis on turning the transmission system into something that requires closer and more inclusive planning, both within regional groupings and across regional lines, may burnish or dim Wellinghoff's legacy.

How the new transmission planning regime will work won't be clear until long after Wellinghoff has left the commission. But that is often the fate of FERC leaders who plow new policy ground.

Perhaps not far behind Order No. 1000 in importance, and a potentially significant Wellinghoff legacy, was FERC Order No. 745, adding to its prior Order 719, that in organized markets demand response resources must be compensated for the service they provide to the market at the locational marginal price for energy.

Return to Top
Electricity Policy

The name game begins for replacement of FERC Chairman Jon Wellinghoff

May 31, 2013

By Kennedy Maize

May 31, 2013 – With Jon Wellinghoff's tenure at the Federal Energy Regulatory Commission coming to an end, who will replace him as chairman and as a third Democrat on the commission? The name game has already begun.

The "inside the Beltway" front runner to replace Wellinghoff as chairman is John Norris. He's a dedicated Democrat, former chairman of the Iowa Utilities Board, and former chief of staff for Agriculture Secretary Tom Vilsack. He has been a diligent FERC commissioner and carved out a niche on the issue of reforming formula transmission tariffs. But Norris has detractors. One veteran energy industry observer says, "Norris talks too much and says too little" at commission public sessions.

A leading outside candidate for appointment to the commission, and perhaps to be named chairman, is Colette Honorable, chair of the Arkansas Public Service Commission. A black lawyer from Little Rock, she's been active in state politics as a Democrat and a player in the machinations of the National Association of Regulatory Utility Commissioners. She's been mentioned in several press accounts as a likely appointee.

Another outsider, who hasn't drawn much attention but who has ties to Senate Majority Leader Harry Reid (D-Nev.), is Rose McKinney-James. She is also a black lawyer, who served on the Nevada Public Utility Commission and was chairman of the state's Department of Business and Industry. She's the principal of a private Las Vegas firm, Energy Works LLC, and serves on the board of directors of both the Energy Foundation and the American Council for an Energy Efficient Economy. According to the ACEEE web site, she served on the 2008-2009 Obama administration transition team and was the lead on FERC issues.

Return to Top
Inside FERC
June 3, 2013

Reliability could play key role as states eye potential legal challenges to ROFR laws

The need to maintain system reliability could play a major role in states' defense of laws designed to provide incumbent utilities the right to build certain transmission lines, as observers say that such considerations could help those laws withstand scrutiny in the event of all-but-certain legal challenges.

The ideas are emerging as more states are pursuing laws that offer some protection of incumbent utilities' right to build certain transmission lines without competing with other developers, also called their right of first refusal, in the face of FERC's implementation of Order 1000.

Under the rule, FERC largely eliminated incumbent utilities' ROFRs. In recent comments defending the commission's decision, Chairman Jon Wellinghoff said that "I don't believe a state could say only an incumbent can build in the state, period."

Said Wellinghoff, "I believe that's a violation of the Commerce Clause. And I think a non-incumbent who had a plan approved by a regional entity could take that state to court. I think they'd have a very good case."

While FERC in Order 1000 said that nothing in the rule "is intended to limit, preempt, or otherwise affect state or local laws or regulations with respect to construction of transmission facilities," the National Association of Regulatory Utility Commissioners recently charged that FERC had gone beyond its original intent to remove federal ROFRs and had taken steps that infringe on state authority (IF, 27 May, 1). In doing so, NARUC expressed concern over Wellinghoff's comments and pointed to FERC's actions in recent orders on Order 1000 compliance filings.

In recent petitions for reconsideration, NARUC argued that FERC erred in its directives to remove references to state law from the tariffs of PJM Interconnection, Midcontinent Independent System Operator and South Carolina Electric and Gas.

At the same time, a growing number of state legislatures are examining and enacting laws that create some sort of state ROFR, with Oklahoma and Indiana most recently passing such provisions.

But in a presentation to a National Regulatory Research Institute webinar May 29, NRRI General Counsel Rishi Garg found that the ROFR law passed in Oklahoma as well as laws approved in Minnesota and the Dakotas in recent years are "facially discriminatory" under the US Constitution's dormant Commerce Clause, a legal construct that bars states from "unjustifiably" discriminating against or burdening interstate commerce.

As such, this would subject those laws to what is called the strict scrutiny standard, Garg said, which holds that such laws are invalid unless they can be "justified by a factor other than economic protectionism" and if the state can show that there was no other means to advance its interest.

In asking what "legitimate state interest" is being protected in such laws, Garg suggested that states analyze whether a competitive solicitation model for transmission development or an approach that prefers incumbents would be better for its state and ratepayers, taking into account potential impacts on the reliability of its grid, economic and public policy goals and other considerations.

This type of analysis could help a state ROFR law withstand a court challenge under strict scrutiny, Garg said. In an earlier interview, Garg noted that it is not beyond the realm of the possible that a court considers reliability considerations as legitimate and justified state interests.

In response to a question on the potential for reliability to be a state interest in a dormant Commerce Clause defense, Suffolk University law professor Steven Ferrey said on the call that most dormant Commerce Clause exceptions deal with things that need to be quarantined, which cannot be easily applied to electricity.

But Ferrey said that reliability is an "excellent consideration" for states looking at these issues, and if the states handle the matter correctly and do not use reliability arguments to veil other motives, then the argument could be in play.

In an interview after the call, Ferrey pointed to several pending cases where both the dormant Commerce Clause as well as the Supremacy Clause — under which a state's law can be found to

be beyond state authority — are in play and involve both power issues and challenges to state actions.

Those included Rocky Mountain Farmers Union v. Goldstene, which is on appeal and currently awaiting a ruling in the 9th US Circuit Court of Appeals, which dealt California's low carbon fuel standard; Entergy Nuclear Vermont Yankee v. Shumlin, on appeal before the 2nd US Circuit Court of Appeals, which pertains to the state's efforts to shutter the nuclear plant; and PPL EnergyPlus, et al. v. Solomon, et al., pending before the US District Court for the District of New Jersey, which is considering New Jersey's Long-term Capacity Agreement Pilot Program.

Ferrey also pointed to a May 20 US Supreme Court ruling in City of Arlington, Texas, et al., v. Federal Communications Commission, et al., in which the court ruled that the FCC could decide the scope of its authority under statute rather than just substantive matters within that authority, so long as it is reasonable.

In the 6-3 decision, the high court invoked the framework created under its 1984 decision in Chevron v. Natural Resources Defense Council, wherein courts defer to an agency's action in cases where the statute is silent or ambiguous and when the agency's justification is found to be a permissible construction of the statute.

In this case, the high court affirmed the lower court ruling, which held that "courts must apply the Chevron framework to an agency's interpretation of a statutory ambiguity that concerns the scope of the agency's statutory authority (i.e.,its jurisdiction)," according to the ruling.

What is noteworthy about the Arlington decision for potential challenges to ROFR issues, Ferrey said, is that both the Federal Power Act and the Communications Act of 1934, the law which FCC implements, are quite old and give states the authority to site and construction infrastructure.

For independent adjudicatory agencies like FERC and the FCC, Ferrey said, the court's finding that Chevron applies in this manner provides some latitude as long as your actions constitute a "reasonable interpretation" of the statute. As such, FERC's determination is entitled to some deference as to the breadth of its authority, including perhaps what is and is not included in tariffs.

While states could conceivably argue that FERC actions are impinging on its FPA-derived authority over construction of transmission lines, the commission could argue in response that ROFR-related actions fall within the scope of its jurisdiction because of their potential impact on rates.

Bobby McMahon

Return to Top

Electric

Megawatt Daily
June 3, 2013

DR participation falls in PJM capacity auction

Bucking the trend of the past two years, the amount of demand response offered and cleared fell this year in the PJM Interconnection's annual capacity auction. Experts said PJM's pursuit of new rules for demand response may have had a dampening effect on offers while the lower prices in this year's auction limited how much demand response cleared.

The results of PJM's annual capacity auction for delivery year 2016/2017, also known as the reliability pricing model's base residual auction, were announced May 24 and showed sharp

From: [redacted]
Sent: Monday, June 03, 2013 7:33 AM
To: [redacted]; Edward Franks; [redacted]; Cynthia Pointer; [redacted]; Joseph McClelland; [redacted]
Subject: Fwd: Current Situation Report, 5/31
Attachments: 05-31-2013 Current Situation Report.pdf

Greetings,

Attached is last week's Current Situation Report, including the following articles:

- ICS-CERT Issues Advisory for Vulnerability in the 3S CODESYS Gateway Application

- Lofty Perch President Mark Fabro Discusses Importance of Developing a Security Culture

- Department of Justice Deputy Attorney General James Cole Suggests Cybersecurity Practices

- FERC Chairman Jon Wellinghoff Announces Resignation

- Electric Power Research Institute's Annabelle Lee on Cryptographic Key Management

- Bipartisan Commission Releases Report on Impacts of International Intellectual Property Theft

- The Basics of Quantum Cryptography Discussed in *The Economist*

Best regards,

[redacted]

Current Situation: Energy Delivery Systems Security

Prepared by Energetics Incorporated for the National SCADA Test Bed Program (NSTB)

May 31, 2013

Vulnerabilities and Cyber Incidents

- **ICS-CERT Issues Advisory for Vulnerability in the 3S CODESYS Gateway Application,** http://ics-cert.us-cert.gov/advisories/ICSA-13-142-01. A denial-of-service vulnerability was identified by independent researcher Nicholas Miles, which may allow an attacker to remotely crash the Gateway server application or execute arbitrary code if exploited. 3S has developed an update to mitigate the vulnerability.

Events and Interviews

- **Lofty Perch President Mark Fabro Discusses Importance of Developing a Security Culture,** http://www.theregister.co.uk/2013/05/23/scada_security/. Speaking at AusCERT 2013, Fabro discussed how SCADA operators play a role in defending against attackers because they can notice unusual processes that occur and take some sort of action. At the same time, personnel can be the tipping point for an intrusion, where an individual may perform an inappropriate action such as inadvertently clicking on a malicious link.
- **Department of Justice Deputy Attorney General James Cole Suggests Cybersecurity Practices,** http://www.networkworld.com/community/node/83098. Speaking at the Georgetown Cybersecurity Law Institute, Cole said that companies and the government can work together to combat cyber threats through prevention, preparedness, and incident response. He discussed other areas that companies should consider, including education, information sharing, and financial obligation to stakeholders.

Federal Agency Cybersecurity Programs and Hearings

- **FERC Chairman Jon Wellinghoff Announces Resignation,** http://www.powermag.com/POWERnews/FERC-Chair-Wellinghoff-Announces-Resignation_5674.html. Wellinghoff's term ends June 30, and is expected to remain as chair at least until a replacement has been confirmed by the Senate. Wellinghoff was appointed as commissioner in 2006 and named chairman in 2009. During his tenure, FERC implemented changes to confront cyber attacks and boost infrastructure investment.

Reports and Surveys

- **Electric Power Research Institute's Annabelle Lee on Cryptographic Key Management,** http://online.electricity-today.com/doc/electricity-today/et_may_2013_digital/2013051701/#42. The May issue *of Electricity Today Magazine* includes an article by Lee, which provides an overview of the variety of data protections that cryptography can provide, along with considerations for applying cryptographic key management systems to advanced metering infrastructure.
- **Bipartisan Commission Releases Report on Impacts of International Intellectual Property Theft,** http://www.forbes.com/sites/emmawoollacott/2013/05/23/us-should-get-tough-on-chinese-ip-theft-committee-warns/. Developed by the Commission on the Theft of American Intellectual Property, the report discusses how cyber espionage is a growing problem and how long supply chains present a challenge to identifying exploited technologies. The report provides over 20 short, mid, and long term

recommendations to mitigate IP theft. *The IP Commission Report* can be found here: http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Other Related-Cyber Issues

- **The Basics of Quantum Cryptography Discussed in *The Economist*,** http://www.economist.com/news/science-and-technology/21578358-eavesdropping-secret-communications-about-get-harder-solace. The article provides an overview of quantum cryptography methods as well as various activities underway, including the pocket-sized QKD transmitter being developed by Los Alamos National Laboratory.

No Relevant News Items for These Categories:

- Standards and Policies
- Cyberwar and Cyberterrorism
- Training, Education, and Collaboration

From: [redacted]
Sent: Wednesday, July 02, 2014 3:09 PM
To: David Andrejcak
Cc: Joseph McClella[redacted]
Subject: Congressional Research Service report
Attachments: CRS-Report-Physical-Security-of-the-U.S.-Power-Grid.pdf

This is the report identified in today's newsclips.

Read it after the holiday unless you need to increase you blood pressure.

[redacted]

84R

Congressional Research Service
Informing the legislative debate since 1914

Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

June 17, 2014

Congressional Research Service
7-5700
www.crs.gov
R43604

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

In the United States, the electric power grid consists of over 200,000 miles of high-voltage transmission lines interspersed with hundreds of large electric power transformers. High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid. HV transformers are also the most vulnerable to intentional damage from malicious acts. Recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security initiatives by utilities and federal regulators. Legislative proposals, notably the Grid Reliability and Infrastructure Defense Act (H.R. 4298 and S. 2158), would expand these efforts by strengthening federal authority to secure the U.S. grid.

For more than 10 years, the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, security standards, grid security exercises, and other measures. There has been some level of physical security investment and an increasing refinement of voluntary grid security practices across the electric power sector for at least the last 15 years. Several major transmission owners have recently announced significant new initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack.

On March 7, 2014, the Federal Energy Regulatory Commission (FERC) ordered the North American Electric Reliability Corporation (NERC) to submit to the Commission new reliability standards requiring certain transmission owners "to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation" of the power grid. In its order, FERC states that physical security standards are necessary because "the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks." According to FERC's order, the new reliability standards will require grid owners to perform risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks.

There is widespread agreement among state and federal government officials, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks would require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true vulnerability of the grid to a multi-HV transformer attack remains an open question. Incomplete or ambiguous threat information may lead to inconsistency in physical security among HV transformer owners, inefficient spending of limited security resources at facilities that may not really be under threat, or deployment of security measures against the wrong threat.

As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several key issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, and recovery from HV transformer attacks.

Contents

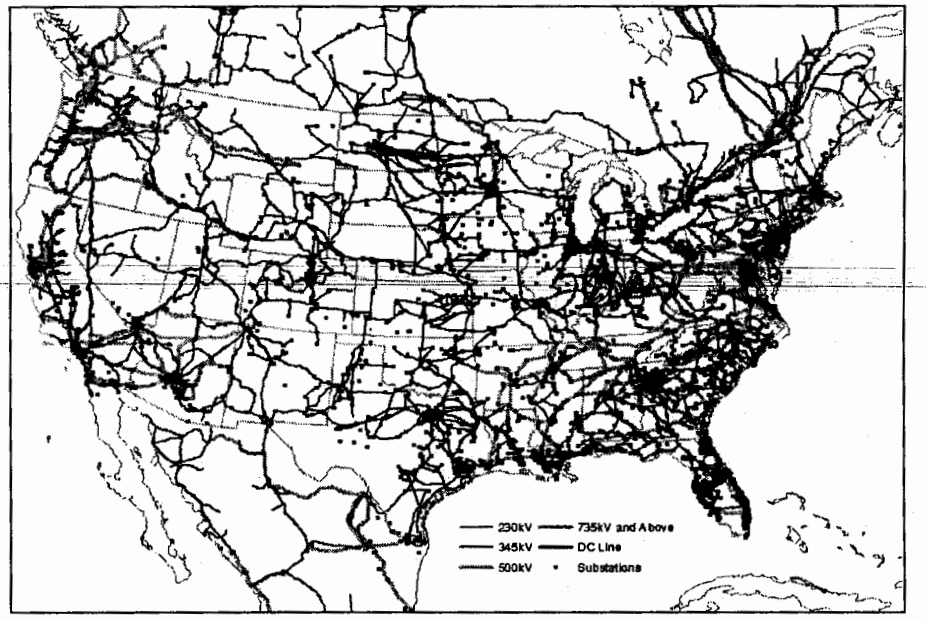
Figures

Contacts

Introduction[1]

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver electric power to consumers. In the United States, this system consists of over 9,000 electric generating units connected to over 200,000 miles of high-voltage transmission lines strung between large towers and rated at 230 kilovolts (kV)[2] or greater.[3] This network is interspersed with hundreds of large electric power transformers whose function is to adjust electric voltage as needed to move power across the network (**Figure 1**). High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60%-70% of the nation's electricity.[4] Because they serve as vital transmission network nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid.

Figure 1. Electric Transmission Network



Sources: CRS analysis of GIS data from Platts, HSIP Gold 2013 (Ventyx), and Esri.

[1] Portions of this report were drawn from CRS Report R42795, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, by Amy Abel, Paul W. Parfomak, and Dana A. Shea.

[2] 1 kV=1,000 volts.

[3] North American Electric Reliability Corporation, "Understanding the Grid," fact sheet, August 2013, http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf. Note that there is no industry consensus as to what voltage rating or other operating characteristic constitutes "high voltage." This report uses 230 kV as the high voltage threshold, but other studies may use a different threshold, such as 115/138 kV, or may include an additional "extra high voltage" category above 345 kV. See, for example, U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014, p. 4.

[4] C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997; William Loomis, "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies," Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL, December 10-11, 2001.

The U.S. electric power grid has historically operated with such high reliability that any major disruption, either caused by weather, operational errors, or sabotage, makes news headlines. Such outages can have considerable negative impacts on business, government services, and daily life. Notwithstanding its high reliability overall, the U.S. power grid has periodically experienced major regional outages. Recent examples include the Northeast Blackout of 2003 (which affected 55 million customer in eight states and Canada) and extended outages in the New York/New Jersey area after Superstorm Sandy in 2012.

Congressional Interest

The various parts of the electric power system are all vulnerable to failure due to natural or manmade events. However, for reasons discussed below, HV transformers are considered by many experts to be the most vulnerable to intentional damage from malicious acts. Congress has long been concerned about grid security in general, but recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers, among other specific aspects of the grid.[5] They have also prompted new grid security initiatives by utilities and federal regulators. Recent legislative proposals, notably the Grid Reliability and Infrastructure Defense Act (H.R. 4298 and S. 2158), would expand these efforts by strengthening federal authority to secure the U.S. grid. The physical security of HV transformers and associated policy issues are the subject of this report.

HV Transformer Risks and Vulnerability

The main risk from a physical attack against the electric power grid—primarily towers and transformers—is a widespread power outage lasting for days or longer. Utilities regularly experience damage to transmission towers due to both weather and malicious activities and are able to recover from this damage fairly rapidly. Thus, while occasionally causing blackouts, physical attacks on towers generally have not resulted in widespread or long-lasting outages. Likewise, the power industry has experienced mechanical failure of individual HV transformers within a single control area resulting in blackouts lasting hours. However, no region in the United States has experienced simultaneous failures of multiple HV transformers. Experts have long asserted that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. This section discusses in more detail HV transformer characteristics and physical security risks associated with them.

High Voltage Power Transformers

Utility transformers control the voltage of electricity so that it can be synchronized with other power supplies, transmitted long distances, and distributed to customers. Transformers range in size from small, pole-mounted units that may serve a dozen homes to transmission units that serve an entire city. The larger the transformer, the higher the voltage the transformer can handle.

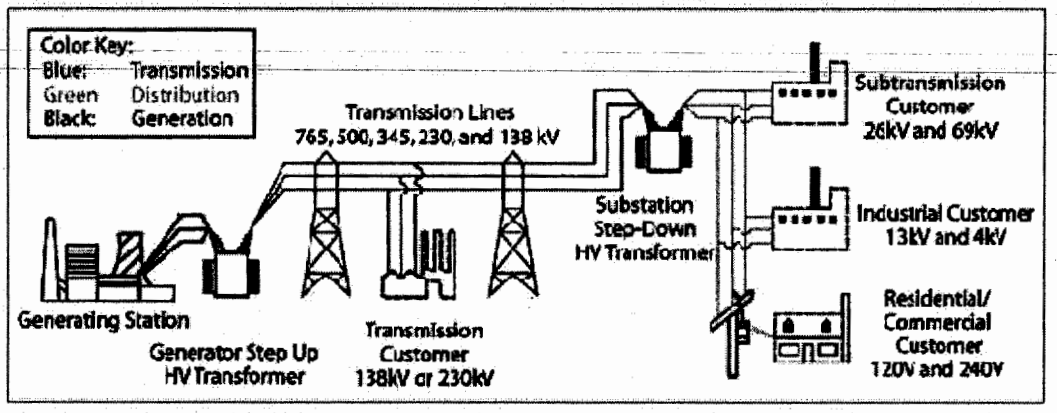
[5] See, for example: Senators Dianne Feinstein, Al Franken, Ron Wyden, and Harry Reid, letter to the Honorable Cheryl LaFleur, Acting Chairman, Federal Energy Regulatory Commission, February 7, 2014, http://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf.

Utility transformers, regardless of size, fundamentally consist of copper wire wrapped around a metallic "core" within an insulated protective housing covered with a 5/8 to 3/4-inch mild steel tank. They are linked to the power grid by protruding metal and (usually) ceramic connectors called "bushings" which resemble giant spark plugs. Larger transformers generate waste heat during operation, so they are cooled by a system of internally circulating oil and external radiators, analogous to the cooling system in a car engine. Transmission transformers are located in network substations along with transmission lines, associated electric equipment, and system controls. These substations may be found in remote locations or near urban centers, depending upon regional transmission needs. Many are located alongside electric generation plants, linking those plants to the grid.

Voltage Management in the U.S. Power System

Electricity produced at U.S. generating stations is converted into a set of three alternating electric currents called three-phase power.[6] The first step in delivering this power is transforming it from the generated voltage (typically 15-50 kV) to higher voltage (138-765 kV), allowing transmission over long distances in greater volumes most efficiently (**Figure 2**).[7] This initial voltage step-up occurs by means of transformers located at transmission substations adjacent to the generating facilities. (The three phases of power are carried separately over three wires on transmission towers.) Close to the ultimate consumer, the power is stepped-down at another transformer substation to lower voltages, typically 13 kV or less. At this point, the power is considered to have left transmission and entered the local distribution system.

Figure 2. Step-Up and Step-Down HV Transformers in the Grid



Source: Adapted by CRS from: U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, Figure 2.1.

High-voltage transformers, especially units above 345 kV, are physically large and extraordinarily heavy. For example, **Figure 3** shows a new 345 kV transformer many times larger than the pickup truck parked alongside. This transformer unit weighs 435 tons, including 29,000 gallons of cooling oil.[8] (Note that the vertical bushings are not yet connected to transmission lines because the unit is being moved.) This is a three-phase unit, with one bushing for each of the three phases. Some substations alternatively employ separate single-phase transformers in sets of three.

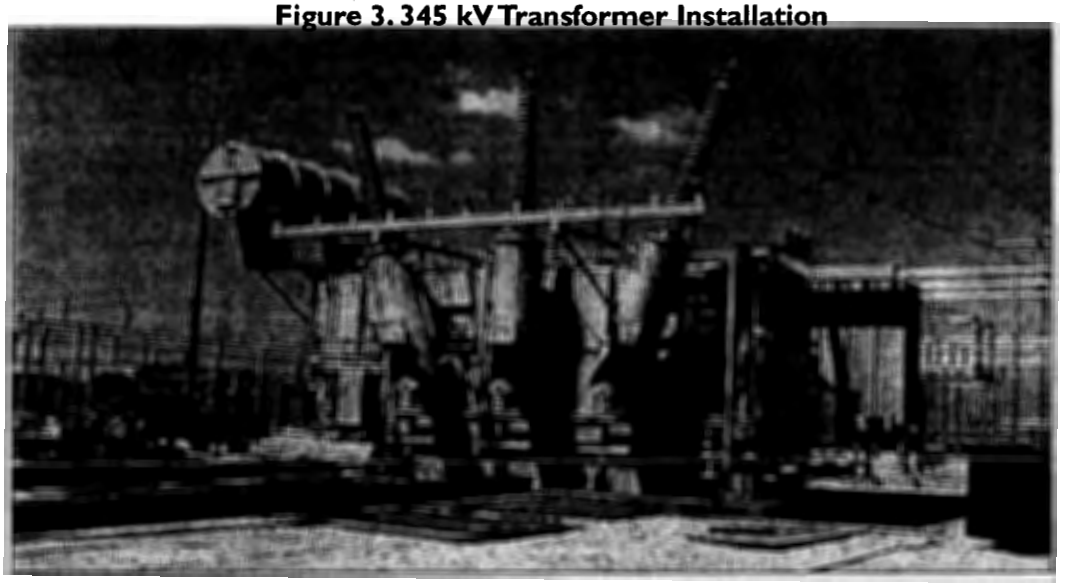
[6] The three currents are sine wave functions of time with the same frequency (60 Hertz). The phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the phases is always nearing a peak.

[7] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

[8] Pauwels Canada, Inc., personal communication, October 20, 2003.

Generally, the higher the transformer's voltage, the larger the transformer. A three-phase 765kV transformer could be 45 feet tall and occupy a footprint of 2,200 square feet—about the size of an average new single-family house.[9]

Figure 3. 345 kV Transformer Installation



Source: Courtesy of Pauwels Canada, Inc., 2003.

Manufacture and Cost

Most HV transformers are unique and therefore are designed and manufactured to custom specifications for a specific network application. In 2010, the lead time between an HV transformer order and delivery ranged from 5 to 12 months for U.S. manufacturers and 6 to 16 months for foreign manufacturers, although lead times well over 20 months could be required in certain situations.[10] This process may include three to four months for the engineering design alone.[11] Since manufacturing generally occurs on a single production line with just-in-time component supplies, advanced production scheduling is important for managing delivery. Physical assembly is labor intensive, requiring manual winding of the copper wire around the transformer core and frequent engineering checks during manufacturing. Extensive testing of completed units also contributes to HV transformer manufacturing time.

The installed cost for an HV transformer depends heavily on its configuration and specific design requirements. New HV transmission substations can cost well in excess of $10 million, including the cost of transformers and other station equipment. According to the U.S. Department of Energy (DOE), the factory prices for HV transformers typically range from $2 million for a 230 kV unit to $7.5 million for a 765 kV unit, before transportation and installation costs.[12]

[9] U.S. Department of Energy, April 2014, p. 7.

[10] U.S. Department of Energy, April 2014, p. 9.

[11] Pauwels Canada, Inc., October 20, 2003.

[12] U.S. Department of Energy, April 2014, p. 7.

U.S. Manufacturing Capability

From 1950 to 1970, utility construction of large generation plants and associated transmission networks fueled a robust U.S. manufacturing market for large transformers. During this period, the United States (and Canada) accounted for approximately 40% of global demand for such units.[13] After 1970, however, utility investment in transmission infrastructure began falling off due to perceived overcapacity, public resistance to transmission siting, and greater regulatory scrutiny of capital expenditures. Beginning in the late 1980s, uncertainty about industry restructuring and the introduction of competition made grid owners even less willing to invest in new transmission. This decline in U.S. transmission investment greatly reduced domestic demand for large transformers, especially HV transformers. By the late 1990s, the United States and Canada accounted for only 20% of global large transformer sales.[14] Demand in the United States has subsequently increased, however. For example, between 2005 and 2013, the total value of large transformers (including medium- and high-voltage units) imported to the United States more than doubled, from $284 million (363 units) to $676 million (496 units).[15]

At the same time, global demand for transformers continued to grow and more foreign manufacturers entered the market. According to U.S. industry representatives, many of these foreign manufacturers benefited from dramatically lower labor costs, so they could underbid U.S. transformer makers for the remaining U.S. demand. Some of these foreign manufacturers may have been protected by import barriers which effectively closed their home markets to U.S. transformer imports. Today, there is limited manufacturing capacity in the United States for HV transformers. Five U.S. facilities state that they can manufacture transformers rated 345 kV or above, although it is not clear how many units in this range they have actually produced. Canada and Mexico have five additional HV manufacturing plants.[16] While limited domestic HV transformer manufacturing may increase delivery time, utilities have not reported difficulty in obtaining needed equipment.

HV Transformer Sites in the United States

There are several thousand HV transformers operating in the United States. Approximately 2,100 are very large units rated 345 kV and above.[17] Investor-owned utilities own most of these, although public utilities such as the Power Marketing Administrations (i.e., Bonneville Power Administration and Western Area Power Administration), Tennessee Valley Authority, and the Los Angeles Department of Water and Power own many HV transformers as well.[18] HV transformer substations are distributed throughout the electric grid, as shown in **Figure 1**, with the greatest number in the eastern part of the country.

---

[13] C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997.

[14] C. Newton, September 1, 1997.

[15] U.S. Department of Energy, April 2014, p. 27.

[16] Kenneth Friedman, U.S. Department of Energy, "DOE Update on GMD/EMP-Related Activities," Presentation to the Geomagnetic Disturbance Task Force Working Group, North American Electric Reliability Corporation, November 13, 2013.

[17] John Kappenman, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, Meta-R-319, Metatech Corp., prepared for Oak Ridge National Laboratory, January 2010, p. 1-14, http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf.

[18] HV substation information for specific investor-owned utilities is publicly available in annual reports filed with the Federal Energy Regulatory Commission (FERC Form-1).

Criticality of HV Transformers

Because they carry so much electricity, the destruction of HV transformers can seriously reduce the transmission capacity of a regional electric power grid and lead to extended blackouts. The impact of such a failure would depend on the electricity flows in that part of the grid, congestion from major network bottlenecks, and the status of other key facilities such as power plants, transmission lines, and other substations. Power grid planners generally anticipate the possible loss of a single HV transformer substation and are prepared to reroute power flows as necessary to maintain regional electric service. But the simultaneous loss of multiple HV transformers, especially in a constrained transmission area, could exceed the capability of a regional network to reroute power through secondary lines.[19]

Numerous publicly available studies have analyzed the risks of a multiple HV transformer failure. For example, the Congressional Office of Technology Assessment (OTA) in a 1990 report on the physical vulnerability of the electric power system found that

> In most cases, the nearly simultaneous destruction of two or three transmission substations would cause a serious blackout of a region or utility, although of short duration where there is an approximate balance of load and supply.... The destruction of more than three transmission substations would cause long-term blackouts in many areas of the country.[20]

In such an emergency scenario, limited electric service could likely be restored in the short term by imposing "rolling" blackouts, rerouting transmission, and using portable transformers. Nonetheless, the loss of key HV substations would leave the regional network crippled and highly susceptible to further disturbance and cascading failure.[21] According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV substation disruption. These areas may have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations. According to press accounts, a FERC power flow analysis in 2013 identified 30 such critical HV transformer substations across the continental United States; disabling as few as nine of these substations during a time of peak electricity demand reportedly could cause a "coast-to-coast blackout."[22] Not all industry experts agree on the potential severity and duration of a blackout from a multi-transformer attack, however, although it is generally accepted that severe outages may be technically possible.[23]

Physical Vulnerability of HV Transformers

All HV transformers are designed to withstand operational risks such as lightning strikes, hurricanes, and network power fluctuations—but they are vulnerable to intentional physical attacks. Despite their great size and internal complexity, HV transformers can be readily disabled or destroyed. According to one manufacturer, "if someone were to intentionally try ... it is a

[19] National Research Council (NRC), *Terrorism and the Electric Power Delivery System*, 2012, p. 69.

[20] Office of Technology Assessment (OTA), *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990, p. 37.

[21] See, for example, Réka Albert, István Albert, and Gary L. Nakarado, "Structural Vulnerability of the North American Power Grid," *Physical Review E*, Vol. 69, 025103(R), 2004.

[22] Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack," *Wall Street Journal*, March 12, 2014.

[23] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal*, February 5, 2014.

surprisingly simple task and there are a large number of ways to conceivably damage a transformer beyond repair."[24] Transformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage. Such attacks can cause massive electrical short circuits and oil fires that would destroy an HV transformer and damage surrounding infrastructure. One fire at a 345 kV substation in Texas, for example, destroyed the transformer and burned for five hours, causing "plumes of smoke that could be seen for miles."[25] In addition to direct attacks on the transformers themselves, HV substations can be further disabled by damaging associated transmission lines or control centers that may be located on site.

Because HV transformers are so big and are connected to the largest overhead transmission towers, they are easily identified along major transmission corridors. High voltage transformers are usually housed in substations that are enclosed with a chain-link fence. Guards are not often stationed at these facilities under normal operating circumstances. Consequently, HV transformers are ordinarily easier to access than other critical electric facilities such as generation plants and control centers. Utilities use closed-circuit surveillance and other methods to detect intrusion. However, access to the substation may be achieved by either cutting or scaling the chain-link fence. Once inside, a saboteur could cause damage by accessing the control room or physically damaging the HV transformer. Penetrating the 5/8 to 3/4-inch steel tank with any device could short-circuit the windings and irreparably destroy the transformer. Alternatively, a saboteur could attempt to open a valve and drain the insulating oil. Igniting the oil might cause the transformer to arc and eventually explode. With a clear line of sight, an attacker could also disable transformers from a distance using conventional rifles.

The vulnerability of individual transformer substations has been demonstrated by successful attacks in recent years. In the most serious case, a rifle attack occurred in April 2013 at PG&E's 500 kV substation in Metcalf, CA. In this attack, multiple individuals outside the substation reportedly shot at the HV transformer radiators with .30 caliber rounds, causing them to leak cooling oil, overheat, and become inoperative.[26] In October 2013, the U.S. Justice Department charged an individual with attacks on the transmission grid in Arkansas, including a deliberate fire at Entergy's 500 kV substation in Lonoke County. The fire consumed the substation control house but electrical service was not interrupted.[27] In 2005, at a Progress Energy substation in Florida, a rifle attack ruptured a transformer oil tank, ultimately causing an explosion and local blackout.[28] Other attacks on substation equipment have been reported with some regularity, although most have been attributed to vandals or careless hunters.

It is very difficult to restore a damaged HV transformer substation. As noted above, transmission experts assert that most HV transformers currently in service are custom designed and, therefore, cannot be generally interchanged. Furthermore, at $3-5 million per unit or more, maintaining large inventories of spare HV transformers solely as emergency replacements is prohibitively costly, so limited extras are on hand. The number of spares a utility maintains is increasingly sensitive information, but one regional transmission control area reported in 2007 that it

[24] Mitsubishi Electric Power Products, Inc., personal communication, Warrendale, PA, September 23, 2003.

[25] Lower Colorado River Authority, "August 6 Update on Transformer Fire," ,ress release, Austin, TX, August 6, 2003.

[26] RTO Insider, "Substation Saboteurs 'No Amateurs'," April 2, 2014, http://www.rtoinsider.com/pjm-grid2020-1113-03/.

[27] Chelsea J. Carter, "Arkansas Man Charged in Connection with Power Grid Sabotage," CNN, October 12, 2013; Max Brantley, "FBI Reports Three Attacks on Power Grid in Lonoke County," *Arkansas Times*, October 7, 2013.

[28] Jim Peppard, "Reward Offered in Power Transformer Shooting," WTSP News (Tampa), October 17, 2005.

maintained 29 spares for 188 transformers rated 500 kV on its system.[29] Programs for the sharing of spare HV transformers among multiple utilities are discussed later in this report.

Within the United States, transportation of HV transformers is difficult. Due to their size and weight, most HV transformers are transported on special railcars, each with up to 36 axles to distribute the load. There are fewer than 20 of these railcars in the Unites States rated to carry 500 tons or more, which can present a logistical problem if they are needed in a transformer emergency.[30] Some specialized flatbed trucks can also carry heavy transformer loads over public roadways, but the few such trucks that exist have less carrying capacity and greater route restrictions than the railcars because HV transformers may exceed highway weight limits.

Targeting of HV Transformers

Malicious individuals could, without significant training, identify critical HV transformer locations and time an attack for greatest effect. This could be accomplished with basic knowledge of transmission operations and regional network characteristics drawn from publicly available sources, including electric marketing data indicating constrained areas of the network.[31] As stated in a 2012 National Research Council report, "terrorists could selectively target key equipment, especially large transformers."[32] The OTA report describes such a scenario:

> [One] example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required. However the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.[33]

In 1997, the Irish Republican Army reportedly planned this kind of coordinated attack against six transmission substations in the United Kingdom. Although the attack was prevented, had it been successful it reportedly could have caused widespread power outages in London and the South East of England for months.[34]

It is relatively easy to learn about HV transformer vulnerabilities from engineers and operators experienced with this technology, either domestically or abroad, since the same technology is used in power grids throughout the world. In the past, transformer experts have provided CRS with detailed descriptions of numerous "simple" ways terrorists could destroy HV transformers. General transformer sabotage information is also available on the Internet. One sabotage manual associated with white supremacist groups available online includes the following discussion:

---

[29] David Egan and Kenneth Seiler, PJM Interconnection, "PJM Manages Aging Transformer Fleet," *T&D World*, March 1, 2007.

[30] Tom Daspit, "Schnabel Cars in Service," web page, August 15, 2013, http://southern.railfan.net/schnabel/schnabel_cars.html.

[31] Marija Ilic, Professor, Engineering and Public Policy and Electrical and Computer Engineering, Carnegie Mellon Univ., Pittsburgh, PA, personal communication, September 22, 2003.

[32] NRC, 2012, p.79.

[33] OTA, June 1990, pg. 37.

[34] Stewart Tendler, "IRA Bombers Plotted to Black Out London and South East for Months," *The Times*, London, England, April 12, 1997.

> The power generation and distribution systems of most major Western cities are surprisingly vulnerable.... Attacking during peak consumption times (Winter in cold climates and Summer in hot climates) will make power diversion impossible.... Arson, explosives or long-range rifle fire can be used to disable substations, transformers and suspension pylons. A simultaneous attack against a number of these targets can shut down power ... with the advantage that service cannot be quickly restored by diverting power from another source. Each broken link in the power grid must be repaired in order to fully restore service. An individual, equipped with a silenced rifle or pistol, could easily destroy dozens of power transformers in a very short period of time.[35]

Security analysts and other industry officials acknowledge that the vulnerability of HV transformers in general is widely known, although understanding the criticality of particular assets within the power grid would require more dedicated effort.

Physical Security Measures for HV Transformers

Although HV transformers are relatively large and often exposed, frequently in rural areas, there are a number of measures available to help prevent an intentional physical attack against a transformer substation. Many of these measures are employed for public safety and to protect against theft, so they may serve multiple purposes. Although security measures appropriate for a particular substation vary depending upon its particular configuration and operating profile, such measures fall into a set of general categories:

- **Protecting information** about critical HV substations, such as engineering drawings, power flow modeling runs, and site security information, which could be useful to a potential attacker.
- **Surveillance and monitoring** through the use of video cameras, motion detectors, imaging, acoustical monitors, aerial drones, and periodic inspection by security employees.
- **Restricting physical access,** such as limiting entry only to necessary employees, installing electronic locks and other access controls, and erecting physical barriers and controls for vehicle entry. Posting full-time guards may also be an option in some circumstances.
- **Shielding assets** from offsite attacks using visual barriers such as opaque or hardened fencing, erecting taller fences, or erecting protective walls.
- **Modifying substation designs** to make them more resistant to physical damage, for example, by strengthening transformer cooling systems or bushings. Reconfiguring substation layouts to limit asset visibility or limit the spread of fire may also be options.

Industry and federal efforts to promote the deployment of such physical security measures are discussed later in this report. In addition to these categories, other measures can help to mitigate the immediate effects of a successful attack ("resiliency"), or to speed full system recovery from such an attack. Measures to enhance the cybersecurity of substation information and control

[35] Axl Hess (a.k.a. Aquilifer), *White Resistance Manual V2.4*, 2001. See also Herschel Smith, "A Terrorist Attack That America Cannot Absorb," captainsjournal.com, blog, September 28, 2010, http://www.captainsjournal.com/2010/09/28/a-terrorist-attack-that-america-cannot-absorb/.

systems, especially supervisory control and data acquisition (SCADA) systems are an important component of power grid security and are usually coordinated with physical security measures.

Sector Initiatives for HV Transformer Security

Over the last decade or so the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, security standards, grid security exercises, and other measures discussed below.

Coordination and Information Sharing

The *National Infrastructure Protection Plan* (NIPP), initially published by the Department of Homeland Security in 2006, "outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes."[36] The plan organizes critical infrastructure into distinct sectors, designating a federal department or agency as the lead coordinator for each sector—the Sector Specific Agency (SSA). Under the NIPP and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, the Department of Energy (DOE) is designated as the SSA for the Energy Sector, which includes the electric utility industry (excluding nuclear power plants). As an SSA, the department is responsible for working with the Department of Homeland Security (DHS), other federal agencies, critical infrastructure owners, independent regulators, and other agencies to implement national policy on critical infrastructure security and resilience.[37] The NIPP also establishes a sector partnership model including private and government coordinating councils:

- The **Electricity Subsector Coordinating Council (ESCC),** initially established in 2004, was organized and administered by companies in the electric power industry to meet regularly to coordinate policy-related activities designed to "improve the reliability and resilience of the electricity subsector, including physical and cyber infrastructure."[38] Through August 15, 2013, the ESCC was chaired by the North American Electric Reliability Corporation (NERC), the not-for-profit organization responsible for ensuring the reliability of the North American grid.[39] The ESCC has since transitioned to a new structure led by electric utility industry executives, although NERC's chief executive officer remains on the ESCC steering committee.[40]

[36] Department of Homeland Security (DHS), "National Infrastructure Protection Plan," web page, April 7, 2014, https://www.dhs.gov/national-infrastructure-protection-plan. The NIPP was mandated under Homeland Security Presidential Directive 7 issued on December 17, 2003.

[37] Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, February 12, 2013.

[38] North American Electric Reliability Corporation (NERC), "Electricity Sub-sector Coordinating Council," web page, April 7, 2014, http://www.nerc.com/pa/CI/Pages/ESCC.aspx.

[39] Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to FERC oversight.

[40] Gerry W. Cauley, North American Electric Reliability Corporation (NERC), letter to U.S. Secretary of Energy Ernest (continued...)

- The **Energy Sector Government Coordinating Council (EGCC),** also established in 2004, is the government counterpart to the ESCC. The EGCC is chaired by the DOE and DHS, incorporating other agencies at all levels of government with interest in energy security. The EGCC plays a key role in implementing the Sector-Specific Plan (discussed below), collaborating with the ESCC to develop and prioritize security programs and initiatives.[41]

In addition to these councils, other organizations have been established with more specific responsibilities related to grid security.

- The **Electricity Sector Information Sharing and Analysis Center (ES-ISAC),** established in 1998, is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.[42] The ES-ISAC is operated by NERC in collaboration with the DOE and ESCC. Members may anonymously share security-related incident information with the ES-ISAC by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.[43]
- NERC's **Critical Infrastructure Protection Committee (CIPC)** coordinates NERC's security initiatives and advises NERC's Board of Trustees, its standing physical and cybersecurity committees, and the ES-ISAC. One of the CIPC's key functions is developing, reviewing, and revising security guidelines; and assisting in the development and implementation of NERC standards.[44]

DOE's Energy Sector-Specific Plan

The 2006 *National Infrastructure Protection Plan* required each critical infrastructure sector to develop a Sector-Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. The section of the DOE's *Energy Sector-Specific Plan* addressing electricity was developed in collaboration with the ESCC and EGCC. The plan identifies high-voltage transformers as an electric sector vulnerability due to their criticality to the power grid and the difficulty of replacing them in the event of a successful attack. Among other measures, the SSP established a goal of implementing "agreements that require participants to maintain transformers for possible sharing in the event of a terrorist act."[45] The plan also identified the "need for a new type of emergency spare (recovery/mobile) high-voltage transformer that can be

(...continued)

Moniz, August 23, 2013, http://www.publicpower.org/files/PDFs/DOESecLetterHistoryESCC.pdf.

[41] Department of Energy, *Energy Sector-Specific Plan*, 2010, p. 20.

[42] The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998.

[43] Electricity Sector Information Sharing and Analysis Center (ES-ISAC), "Frequently Asked Questions," web page, https://www.esisac.com/SitePages/FAQ.aspx.

[44] North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection Committee (CIPC)," web page, http://www.nerc.com/comm/CIPC/Pages/default.aspx, April 8, 2014.

[45] Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 54.

deployed and energized quickly to rapidly recover from outages caused by natural disasters and deliberate attacks."[46]

ESCC's Critical Infrastructure Strategic Roadmap

In November 2010, the Electricity Subsector Coordinating Council published its *Critical Infrastructure Strategic Roadmap* report, to provide a framework for identifying risks that could seriously disrupt the grid and for promoting actions to enhance grid reliability and resilience. The report paid particular attention to "severe-impact risks with the potential to impact large portions of the grid, or disrupt service for an extended period of time."[47] The report considered three principal risk scenarios, including

> **Scenario 1: Physical Attack on Significant Electricity System Equipment**
> A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect [sic] on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.[48]

The report recommended a current capability assessment to prevent and respond to such a scenario as a "high priority." The report also recommended as "important" both a study of "options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g., large high-voltage transformers)" and an initiative to "enhance the availability of critical spare equipment ... starting with high voltage transformers."[49]

Transformer Equipment Programs

Consistent with the recommendations of the studies above, several programs have been instituted within the electric power sector to address the operational issues that emerge due to the scarcity of spare HV transformers and associated equipment in the event of a physical attack or other grid emergency.

DHS Recovery Transformer Program

In 2008, the Department of Homeland Security (DHS) initiated a program to develop a prototype "Recovery Transformer" (RecX) which could enable recovery from transformer failure within days rather than months or longer.[50] The RecX transformer was intended to be adaptable to a range of common grid specifications as well as being smaller, lighter, easier to transport, and quicker to install than conventional HV transformers. The RecX prototype was designed to replace the most common HV transformers (345 kV) used in the U.S. grid.[51] This configuration

---

[46] Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 70.

[47] North American Electric Reliability Corporation (NERC), *Critical Infrastructure Strategic Roadmap*, November 2010, p. 2, http://ccpic.mai.gov.ro/docs/NERC_ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf.

[48] NERC, November 2010, p.18. This scenario involved the loss of three HV substations serving large urban centers with a restoration time to 100% operating capacity of 6-18 months.

[49] NERC, November 2010, pp.19-20.

[50] The program was partly funded by the DHS Science and Technology Directorate in a consortium with the Electric Power Research Institute, CenterPoint Energy, and ABB.

[51] ABB, "US Rapid Recovery Transformer Initiative Succeeds Using Specially-Designed ABB Transformers," press (continued...)

reportedly could be used to replace approximately one quarter of the 2,100 transformers in this voltage class currently deployed.[52] In 2012, the only three single-phase RecX prototype units were installed in an operating 345 kV substation in Texas during a simulated emergency drill. The units remain in operation, having met or exceeded their service requirements. Although the RecX transformers have reliability and efficiency characteristics comparable to other 345 kV transformers, and are also comparably priced ($7.5 million each), the manufacturer had received no orders for commercial production of these units as of February 2014.[53] Having successfully demonstrated the RecX concept, the DHS is no longer funding the RecX program.

EEI Spare Transformer Equipment Program

In 2006, Edison Electric Institute (EEI), the main trade association for U.S. investor-owned electric utilities, initiated its Spare Transformer Equipment Program (STEP) to strengthen "the sector's ability to restore the nation's transmission system more quickly in the event of a terrorist attack."[54] The STEP program requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a "triggering event"—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state of emergency by the President.[55] FERC granted blanket authorization for the transfer and cost recovery of transmission equipment under the STEP program in September 2006.[56] State regulators with jurisdiction over participating utilities have also granted pre-approval for STEP transfers.[57] The program is designed to deal with terrorist events, but it also provides a mechanism for voluntary sharing of transformers in other emergencies, although these may require additional regulatory approvals. EEI requires annual recertification and conducts a STEP program drill every summer to ensure the program and its members will be fully prepared to respond in the event of an actual triggering event.[58]

NERC Spare Equipment Database

In 2012, NERC initiated its Spare Equipment Database (SED) program intended to serve as a tool to "facilitate timely communications between those needing long-lead time equipment damaged

(...continued)

release, October 4, 2012.

[52] Matthew L. Wald, "A Drill to Replace Crucial Transformers (Not the Hollywood Kind)," *New York Times*, March 14, 2012.

[53] National Research Council (NRC), *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*, 2013; Sarah Mahmood, Department of Homeland Security, personal communication, February 10, 2014.

[54] Edison Electric Institute (EEI), "Spare Transformers," web page, April 10, 2014, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

[55] Edison Electric Institute (EEI), "Overview of the Spare Transformer Equipment Program," slide presentation, February 23, 2014.

[56] Federal Energy Regulatory Commission, *Order on Application for Blanket Authorization for Transfers of Jurisdictional Facilities and Petition for Declaratory Order*, Docket Nos. EC06-14-000 and EL06-86-000, September 22, 2006.

[57] EEI, February 23, 2014.

[58] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

in a [High Impact, Low Frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization."[59] The SED program is a confidential web-based catalog of spare transformers rated at 100 kV or higher. Only NERC and the equipment owners can see their spares data (although NERC can make high-level reports to FERC); requests for equipment are double-blind. Participation is voluntary and requires no commitment or mandatory sharing of spares.[60] Unlike EEI's STEP program, however, the SED program has not been granted pre-approval from FERC or state regulators for equipment transfers. Thus, the ability to transfer the ownership of transformers from one company to another may require additional approvals, even during an emergency.

Grid Security Exercises and Simulations

NERC and FERC have conducted grid security computer simulations and exercises specifically incorporating hypothetical attacks on HV transformer substations.

GridEx and GridEx II

In 2011, NERC conducted GridEx 2011, its first electric sector-wide grid security exercise. The exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on HV transformers.[61] Among other findings, the exercise determined that "utilities took appropriate steps to secure the grid."[62] Nonetheless, NERC recommended that "entities should ensure their response protocols address a coordinated threat," and that it would "facilitate and support the development of updated physical security guidance."[63]

After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario, developed using open-source techniques, included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including HV transformer substations.[64] Among other conclusions, NERC's after-action report stated:

> While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.... The extreme challenges posed by the Severe Event scenario provided an

[59] North American Electric Reliability Corporation (NERC), *Special Report: Spare Equipment Database System*, August 2011.

[60] North American Electric Reliability Corporation (NERC), "Spare Equipment Database," slide presentation, NERC Industry Webinar, July 22, 2013, http://www.nerc.com/pa/RAPA/webinardl/SED_Presentation_July_22_2013.pdf.

[61] North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

[62] NERC, 2012, p. ii.

[63] Ibid.

[64] North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

> opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.[65]

NERC did not publicly report details about the overall impacts to the grid or outages in particular regions due to the sensitive nature of such information. Utilities and other agencies participating in the exercise viewed it a useful tool for utilities to test their readiness and preparedness for attacks on the grid.[66]

FERC "Electrically Significant Locations" Study

In early 2013, prior to the Metcalf attack, then-FERC Chairman John Wellinghoff directed FERC staff to prepare an analysis identifying critical HV substations in the North American power grid.[67] Using power flow analysis software to model the impacts to the transmission system from the loss of specific grid assets,[68] FERC staff compiled a list of "Electrically Significant Locations (ESLs)" within the grid.[69] Neither details of the ESL study methodology nor its results have been released publicly by FERC or other agencies, although some findings have been reported in the press and discussed publicly by federal officials. According to the *Wall Street Journal*, the FERC analysis identified 30 critical transformers substations; in FERC's simulation, losing nine of these substations (in various combinations) as the result of a coordinated attack reportedly was found to cause a nationwide blackout for an extended time.[70]

Members of Congress were highly critical of both the *Wall Street Journal* and FERC officials for inappropriately releasing what was perceived to be highly sensitive information about power grid physical vulnerability.[71] A subsequent investigation by the Department of Energy's Inspector General concluded that FERC's handling of the ESL study findings was improper.[72] The protection of information about grid security is further discussed in a later section of this report.

---

[65] NERC, March 2014, p. 5.

[66] See, for example, American Public Power Association, "Physical Security and the Electric Sector," fact sheet, February 2014, http://www.publicpower.org/files/PDFs/PhysicalSecurityIBFebruary2014.pdf; Matthew L. Wald, "Power Grid Preparedness Falls Short, Report Says," *New York Times*, March 12, 2014.

[67] Federal Energy Regulatory Commission (FERC), "Second Set of Responses of the Federal Energy Regulatory Commission to Senator Murkowski's Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee," May 5, 2014, pp. 12-13, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5c3bf9d7-bb7f-4379-8f57-f58881a0b5d6.

[68] FERC staff employed the commission's Topological and Impedance Element Ranking (TIER) model to identify "significant" assets based upon undisclosed criteria. For more details of the TIER model, see Bernard C. Lesieutre et al., "Topological and Impedance Element Ranking (TIER) of the Bulk-Power System," University of Wisconsin—Madison, prepared for the Federal Energy Regulatory Commission, August 2009, https://www.ferc.gov/EventCalendar/Files/20090911112656-TIER%20REPORT.pdf.

[69] Federal Energy Regulatory Commission (FERC), "Response to Senator Murkowski's Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee, Question 39," May 5, 2014, p. 2, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=2826f80a-a986-45d1-9261-87b45e1d6872.

[70] Rebecca Smith, "U.S. Risks National Blackout from Small-Scale Attack on Substations," *Wall Street Journal*, March 13, 2014.

[71] Senate Committee on Energy and Natural Resources, "Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities," press release, March 31, 2014.

[72] U.S. Department of Energy, Office of Inspector General, "Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission," DOE/IG-0906, April 9, 2014.

HV Transformer Security Standards

Several grid security guidelines or standards have been developed or proposed to address the physical security of the grid, including HV transformers. These standards have been promulgated by NERC as voluntary best practices since at least 2002, with subsequent revisions. However, in the wake of the Metcalf incident, FERC has ordered the imposition of mandatory physical security standards in 2014.

IEEE Substation Security Standard

In 2000, the Institute of Electrical and Electronics Engineers (IEEE), a technical professional society, published its first standards for electric power substation physical and electronic security. The voluntary standard addressed "security issues related to human intrusion upon electric power supply substations" and various methods to mitigate them.[73] The standard called for the development of security assessments and, for "high-risk areas," increased security measures such as motion detectors, perimeter/area detection systems, security cameras, physical barriers, and posted guards.[74] However, according to the IEEE, the standard is intended to address security issues related to unauthorized access, theft, and vandalism. The IEEE states that "attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc. are beyond the scope of this standard."[75]

NERC Physical Security Guidance

In June 2002, NERC published its initial guidance for physical response to security alerts from the federal government. This alert system was revised in October 2002 to correspond to DHS's new color-coded threat level system.[76] NERC's guidance was voluntary, intended to provide "examples of security measures that electric utility organizations may consider taking, based on the Alerts issued."[77] NERC's guidance included 35 specific security measures for the five threat DHS levels. These measures ranged from "occasional" workforce awareness programs and annual security plan reviews during times of low threat (green) to continuous monitoring of critical facilities, potentially with armed guards, during times of highest threat (red).[78] Along with this guidance, NERC published initial guidelines for vulnerability and risk assessment to help identify critical facilities and countermeasures to mitigate threats.[79]

---

[73] Institute of Electrical and Electronics Engineers (IEEE), *1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security*, January 30, 2000.

[74] IEEE, January 30, 2000, p. 16.

[75] Institute of Electrical and Electronics Engineers (IEEE), "P1402—Standard for Physical Security of Electric Power Substations," web page, June 3, 2014, http://standards.ieee.org/develop/project/1402.html.

[76] North American Electric Reliability Corporation (NERC), *Threat Alert System and Physical Response Guidelines for the Electricity Sub-sector*, Version 2.0, October 8, 2002, http://www.iwar.org.uk/infocon/threat-levels/tas_physical_V2.pdf.

[77] NERC, October 8, 2002, p. 2.

[78] NERC, October 8, 2002, pp. 3-4.

[79] NERC, *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 14, 2002, http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Vulnerability%20and%20Risk%20Assessment,%20Version%201.0.pdf.

In November 2005, NERC published a third version of its physical security guidelines, to provide "examples of security measures that other electricity sector organizations *should* consider when responding to threat level alerts" [emphasis added].[80] Thus, while still voluntary, these measures appear to have been intended as recommendations rather than considerations as stated in the earlier versions. The 2005 document included 55 measures, including new measures and existing measures expanded or described more specifically. New measures during times of low threat included, for example, annual audits of critical facility access programs and identifying critical facility long-term and short-term security measures (e.g., vulnerability assessments and security barriers).[81]

The Energy Policy Act of 2005 (P.L. 109-58) mandated the implementation of electric grid reliability standards under new authority granted to the Federal Energy Regulatory Commission. FERC subsequently designated NERC as the Electric Reliability Organization certified by the commission to establish and enforce reliability standards for the U.S. electric transmission grid, subject to commission review. In 2008, FERC approved NERC's initial reliability standards for critical infrastructure; however, these standards were developed primarily to address transmission grid cybersecurity, not physical security.[82] Subsequent NERC standards have expanded these cybersecurity requirements.

In October 2013, NERC published its most recent revision to its physical security guidance, *Security Guideline for the Electricity Sub-sector: Physical Security Response,* providing to electricity sector members "actions they should consider when responding to the threat alerts" issued by the DHS.[83] Continuing its voluntary (rather than regulatory) approach to physical security, NERC's guidance states that "each organization decides the risk it can accept and the practices it deems appropriate to manage its risk."[84] This version of NERC's guidance lays out 77 distinct security measures corresponding to three levels of threat: (1) Normal Operations/Best Practices, (2) Elevated, and (3) Imminent.

FERC Physical Security Best Practices

In 2013, FERC staff along with staff from the Federal Bureau of Investigation (FBI), DOE, DHS, and NERC participated in a number of meetings with utilities and law enforcement agencies to discuss immediate findings and recommendations stemming from the Metcalf substation attack. As part of these meetings, FERC staff shared with utilities a list of best practices for physical security. Although the list has not been made public, it reportedly included prescriptive security measures (e.g., outward-facing video surveillance) focused on security threats similar to that experienced at the Metcalf substation.[85] In 2014, DHS, in coordination with FERC, the ES-ISAC,

[80] NERC, *Security Guidelines for the Electricity Sector: Physical Response*, November 1, 2005, p.1, http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Physical%20Response,%20Version%203.0.pdf.

[81] NERC, November 1, 2005, p. 3.

[82] FERC Order 706.

[83] North American Electric Reliability Corporation (NERC), *NERC: Security Guideline for the Electricity Sub-sector: Physical Security Response*, October 28, 2013, p. 1, http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf.

[84] NERC, October 28, 2013, p.1.

[85] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

NERC, the FBI, and industry experts, has convened another series of regional briefings across North America with utilities and law enforcement officials to follow up on the initial outreach regarding substation physical security.[86]

NERC Physical Security Regulations

On March 7, 2014, FERC ordered NERC to submit to the commission within 90 days proposed reliability standards requiring certain transmission owners "to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation" of the power grid.[87] In its order FERC states that physical security standards are necessary because "the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks."[88] According to FERC's order, the new reliability standards must require transmission owners or operators to perform a risk assessment of their systems to identify their "critical facilities," evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against attacks to those identified critical facilities.[89] The order requires that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.[90] The proposed standard applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.[91] The standard consists of six principal requirements (R1-R6), summarized as follows:

R1. Risk assessments by transmission owners to identify critical transmission facilities;

R2. Independent third party verification of risk assessments conducted under R1;

R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;[92]

R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;

---

[86] Gerry Cauley, CEO, North American Electric Reliability Corporation (NERC), letter to Senator Harry Reid, February 12, 2014, p. 2, http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf.

[87] Federal Energy Regulatory Commission (FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf.

[88] FERC, March 7, 2014, p. 2.

[89] FERC, March 7, 2014, pp. 3-4.

[90] North American Electric Reliability Corporation (NERC), Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf.

[91] NERC, May 23, 2014, Exhibit A, p. 1.

[92] A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in section 3 of the Federal Power Act (16 U.S.C. 796).

R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and

R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.[93]

The proposed standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.[94] The new standard would be enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission's enforcement authority and oversight under P.L. 109-58.[95]

Company-Specific Initiatives

Electric utilities have long had an ongoing responsibility to ensure grid reliability, in part through operating practices and investments related to grid safety and security.[96] As the standards in the previous section suggest, there has been some level of physical security investment and an increasing refinement of grid security practices across the electric power sector for at least the last 15 years. Nonetheless, several major transmission owners have recently announced significant new initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack. Other utilities have included new substation security investments in broader initiatives for company security.[97] The following examples illustrate the types of security changes being proposed by these grid owners. Note that other major utilities have not publicly announced similar new security initiatives. A comprehensive review or comparison of physical security plans among all major grid owners in the United States is beyond the scope of this report.

The Tennessee Valley Authority

In February 2012, the Tennessee Valley Authority (TVA) announced that it was "realigning its operations and structure to enhance security at TVA's non-nuclear power facilities ... focusing more of our non-nuclear security resources on our critical infrastructure," including HV substations.[98] The realignment included ending uniformed patrols in favor of installing more security technology, and the stationing of contract guards 24 hours a day at critical facilities. Together with local law enforcement cooperation, the shift to contract guards was intended to

[93] NERC, May 1, 2014, Section B.

[94] NERC, May 1, 2014, p. 14.

[95] Federal Energy Regulatory Commission (FERC), *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

[96] For example, see security discussion in Con Edison, Initial Brief on Behalf of Consolidated Edison Company of New York, Inc. in Support of a Permanent Electric Rate Increase, Before the New York State Public Service Commission, November 30, 2007, http://media.corporate-ir.net/media_files/irol/61/61493/total120507.pdf.

[97] See Southern California Edison, *Safety, Security, & Compliance (SS&C): Volume 4—Corporate Security and Business Resiliency*, 2015 General Rate Case, Before the Public Utilities Commission of the State of California, November 2013, http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/$FILE/SCE-07%20Vol.%2004.pdf.

[98] Tennessee Valley Authority, "TVA Realigns Security to Enhance Protection at Non-Nuclear Assets," press release, February 17, 2012, http://www.tva.gov/news/releases/janmar12/tvap.html.

provide a more persistent security presence and faster incident response at key locations. Among the security technologies reportedly deployed by TVA are "surveillance, infrared cameras, video analytics for alarm verification and assessment, virtual perimeters, card readers, [and] automated gates."[99] TVA's security initiatives in 2012 appear to have been motivated primarily by security concerns such as copper theft, but would be applicable to more serious security risks such as terror attacks. In February 2014, after the Metcalf incident, TVA reportedly stated that it was "intensifying efforts" to educate local law enforcement about the importance of substations, including taking police on site visits to see substations during normal operations.[100] The utility has also been canvassing residents near TVA property asking them to report unusual activity around grid facilities.

Pacific Gas and Electric (PG&E)

In February 2014, in response to the attack on its Metcalf substation, PG&E announced that it would be investing approximately $100 million over three years to improve substation security. Physical security measures mentioned by the company include new perimeter barriers, shielding for certain equipment, more cameras (inside and outside the fence), and clearing vegetation. For its most critical facilities, the company is "studying advanced detection technology such as night vision and thermal imaging."[101] Other security measures mentioned in news reports about PG&E include enhanced lighting, 24-hour security guards, and increased patrols by local law enforcement agencies.[102]

Dominion

In February 2014, Dominion Virginia Power, an operating company of Dominion, announced plans to spend up to $500 million over five to seven years "to harden its transmission substations and other critical infrastructure against man-made physical threats and natural disasters, as well as stockpile crucial equipment for major damage recovery."[103] Dominion reportedly began to increase substation security efforts in 2013, focusing first on substations at greatest risk.[104] Among the security measures identified by the utility are physical barriers, additional access control, equipment design/hardening, polymer bushing installation, additional spare equipment, and relocation of spare equipment to off-site storage areas. Other measures reportedly include dual-perimeter "no man zones" around substations and installing systems for key-card access to substation yards.[105] Dominion's security plan has yet to be approved by Virginia regulators for cost recovery in electric rates.

---

[99] "Addressing Cyber and Physical Risks in Modern Utility Security," *Security*, March 1, 2014, http://www.securitymagazine.com/articles/85275-addressing-cyber-and-physical-risks-in-modern-utility-security.

[100] Rebecca Smith, "U.S. Utilities Tighten Security After 2013 Attack," *Wall Street Journal*, February 9, 2014.

[101] Geisha Williams, Executive Vice President of Electric Operations, Pacific Gas and Electric Company, "PG&E Metcalf Attack: Gunfire on Substation Has Led to Greater Security," *San Jose Mercury News*, April 15, 2014.

[102] "PG&E to Spend $87M on Security to Protect Large Substations from Attack," KTVU, Oakland, CA, February 12, 2014.

[103] Dominion. "Substation Security," fact sheet, Spring 2014, https://www.dom.com/about/electric-transmission/pdf/substation-security-soc-factsheet.pdf.

[104] Tracy Sears, "Troopers Increase Security at Virginia Substations Critical to Grid," WTVR, March 11, 2014.

[105] Peter Bacqué, "Va. Power to Spend Up to $500M on Security Plan," *Richmond Times-Dispatch*, February 8, 2014.

Bonneville Power Administration

In its 2014 draft *Security Asset Management Strategy*, the Bonneville Power Administration (BPA) proposes approximately $37 million in additional capital spending through FY2020 for physical security measures at approximately 60 critical transformer substations.[106] BPA's *Strategy* states that, over the last 13 years, the utility "has conducted hundreds of security and risk assessments using several industry accepted methodologies," and began implementing security improvements based on these risk assessments beginning in 2001.[107]

Issues for Congress

The recent transformer substations attacks, together with federal grid security exercises, have focused attention on the vulnerability of HV transformer substations to organized physical attacks. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several key issues as part of its oversight of the sector.

Identifying Critical Transformers

A fundamental consideration regarding HV transformer security is a clear and stable understanding of which transformers are "critical." The USA PATRIOT Act of 2001 defines "critical infrastructure" in the most general sense as "systems and assets ... so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[108] It its 2009 guidelines for identifying critical assets specifically in the electricity sector, NERC defines critical assets as those "that if destroyed, degraded, compromised (e.g., misused) or otherwise rendered unavailable would unacceptably affect the reliability or operability of the [Bulk-Power System] as a whole.... "[109] FERC's 2014 order mandating physical security standards for the grid defines a "critical facility" as "one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[110] All three definitions associate "criticality" with a failure event of national significance, although none provides a more prescriptive basis for identifying such assets.

In its physical security order, FERC does not require that a "mandatory" number of critical facilities be identified under the standards.[111] Determination of whether a specific HV transformer

[106] Bonneville Power Administration (BPA), *Security Asset Management Strategy*, February 2014, p. 29, http://www.bpa.gov/Finance/FinancialPublicProcesses/CapitalInvestmentReview/2014CIRDocuments/Security%20Full%20Asset%20Strategy%20Final%20Draft.pdf.

[107] BPA, February 2014, p. 31.

[108] P.L. 107-56 § 1016(e).

[109] North American Electric Reliability Corporation (NERC), "Security Guideline for the Electricity Sector: Identifying Critical Assets," September 17, 2009, p. 1, http://www.nerc.com/fileUploads/File/Standards/Reference%20Documents/Critcal_Asset_Identification_2009Nov19.pdf.

[110] FERC, March 7, 2014, p. 3.

[111] FERC, March 7, 2014, p. 3.

is "critical" will be based on each individual asset owner's "objective analysis, technical expertise, and experienced judgment."[112] In its proposed physical security standards, NERC requires transmission owners with HV assets meeting prescriptive criteria to examine whether they *may* have critical transformers, but it is up to the owners to determine themselves if any of their assets *are* critical through a periodic risk assessment based on their own respective transmission analyses, subject to independent validation.[113] Thus, grid owners could have considerable latitude in determining which of their transformer substations (if any) are critical and therefore subject to the requirements of the new standard.

Although there are many candidate transformer substations in the grid, relatively few are likely to be of national significance. As discussed above, of the numerous HV transformer substations in the United States, FERC's 2013 power flow analysis identified only 30 as being critical to the national grid (although each of these substations may contain multiple HV transformers). Whether the number of critical transformer substations under FERC's definition above turns out to be higher or lower than 30, it will likely be only a small fraction of the total asset base. This conclusion is consistent with FERC's expectation that under NERC's new standard "the number of facilities identified as critical will be relatively small.... For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be 'critical' as the term is used in this order."[114] Consistent with this view, the NERC working group responsible for drafting the proposed physical security standard likewise expects the number of critical facilities to be "small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."[115]

Properly identifying which HV transformer substations are critical is a key issue. Otherwise, the electricity sector risks the possibility of hardening too many substations, hardening the wrong substations, or both. Either outcome could increase ultimate costs to electricity consumers without commensurate security benefits, and could potentially divert limited security resources from other important grid priorities (e.g., cybersecurity). Independent verification is intended to validate utility assessments of substation criticality, but the standard's reliance on company-by-company assessments may still allow for important differences in analytic methodology or assumptions, and thus inconsistent conclusions about transformer criticality. Furthermore, company-specific studies may not align with a "top down" assessment of asset criticality like that performed by FERC in its Electrically Significant Location (ESL) analysis. Congress may examine whether company-specific assessments of transformer criticality could differ from national-level assessments and what implications, if any, such differences might have on overall grid security and company efforts to protect particular substations.

Confidentiality of Critical Transformer Information

Ensuring the confidentially of critical infrastructure information has been a long-standing concern across all critical infrastructure sectors. It is a key reason for the establishment of sector Information Sharing and Analysis Centers (ISACs), including the Electricity Sector ISAC, discussed above. Confidentiality also factors into the administration of the industry's spare

[112] FERC, March 7, 2014, p. 3.

[113] NERC, May 1, 2014, p. 30.

[114] FERC, March 7, 2014, p. 3.

[115] NERC, May 1, 2014, p. 28.

transformer programs and other activities related to critical infrastructure. FERC has established policies for the protection of critical energy infrastructure information (CEII) through a series of orders, beginning with Order 630, issued February 21, 2003.[116] The order (§ 27) defines CEII as information that "must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act [FOIA]." It also establishes procedures and responsibilities for determining what information qualifies as CEII and handling CEII requests.[117] FERC's 2014 order mandating physical security standards also requires procedures to ensure confidential treatment of sensitive information.[118]

Press articles in the wake of the Metcalf attacks, notably in the *Wall Street Journal*, cited specific details about FERC's 2013 ESL analysis, reportedly from a copy of a FERC presentation obtained by the paper. Notwithstanding FERC's orders on CEII, Members of Congress and FERC officials have expressed concern that the release of the presentation by FERC staff and the publication of details in the press potentially compromised grid security.[119] Others reportedly have disputed this concern, including the former FERC Commissioner responsible for commissioning and presenting the ESL study findings at industry meetings.[120] In April 2014, the DOE Inspector General concluded that the FERC presentation in question "should have been classified and protected from release" and "that the Commission may not possess adequate controls for identifying and handling classified national security information."[121] The Acting Chairman of FERC has testified that the commission is adopting the Inspector General's recommendations to improve its handling of CEII and requested additional authority from Congress for exemption from FOIA.[122]

FERC staff may be improving the way CEII is safeguarded in response to the Inspector General's report, but securing CEII may continue to be an issue if NERC's new physical security regulations are approved by the commission. NERC's regulations would require independent risk assessments by multiple grid owners and 3rd party validation of those assessments. This process, by construction, would cause considerable new CEII to be created (e.g., multiple Midwest power flow models) and shared among utilities, RTOs, and consultants in ways that may be new to the industry. Ensuring that CEII generated and transferred among these entities remains secure could require special attention. As FERC's improper management of the ESL study information shows, having strong CEII policies in place may not guarantee that those policies will be correctly and uniformly followed—even by the agency that created them.

[116] For an overview, see Federal Energy Regulatory Commission (FERC), "Critical Energy Infrastructure Information (CEII) Regulations," web page, June 28, 2010, http://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp.

[117] Federal Energy Regulatory Commission (FERC), Order No. 630, Final Rule, February 21, 2003, http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9639612.

[118] FERC, March 7, 2014, p. 10.

[119] Senate Committee on Energy and Natural Resources, "Sens. Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities," press release, March 27, 2014; The Honorable Cheryl LaFleur, Chairman (Acting), Federal Energy Regulatory Commission (FERC), Testimony Before the Senate Committee on Energy and Natural Resources Hearing, "Keeping the Lights On—Are We Doing Enough to Ensure the Reliability and Security of the U.S. Electric Grid?," April 10, 2014.

[120] Bobby McMahon, "Wellinghoff Says FERC Analysis of Grid Vulnerability was Public, Calls Review 'Waste of Time'," *Inside FERC*, March 31, 2014, p. 1.

[121] U.S. Department of Energy, Office of Inspector General, "Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission," DOE/IG-0906, April 2014, p. 1.

[122] The Honorable Cheryl LaFleur, Testimony on April 10, 2014.

Adequacy of HV Transformer Protection

The electric power sector has had physical security guidelines in place for well over a decade, as discussed above. These voluntary guidelines have been updated and expanded periodically to reflect industry experience, changes in the security environment, and new technologies. Prior to 2014, however, it appears that the physical security initiatives among grid owners were focused primarily on preventing vandalism and theft (of copper wire) rather than a terrorist attack.[123] As the recent substation attacks in California, Arkansas, and Florida have shown, many other security measures available to grid owners were not implemented—even at critical HV substations.

A grid owner's focus on vandalism and theft may be understandable because such incidents have occurred frequently and their associated costs are tangible and well-understood. Investing in security against a terrorist attack presents a greater challenge in terms of costs and benefits. As a 2006 report from the Electric Power Research Institute states,

> Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.[124]

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers.

The Metcalf incident and GridEx exercises have provided the electric sector with valuable new information about the potential threat, vulnerability, and consequence of a coordinated attack on HV transformers. Risk assessments incorporating this information presumably would justify (with or without a new NERC standard) increased security investments at critical substations to prevent intentional attacks. The recently announced voluntary spending plans at PG&E, Dominion, and BPA for HV substation security appear to reflect such risk and cost-benefit reassessments. Nonetheless, there continues to be considerable uncertainty about the risk of terror attacks on the power grid, and what measures are economically justified in addressing them. PG&E, BPA, and the other utilities announcing large security investments have already decided to make such investments, but they are in the minority. Other major owners of critical HV transformers have not publicly announced similar plans.

NERC's proposed standards for power grid physical security would ensure considerable consistency in the *process* utilities must undertake to identify critical substations and develop plans to secure them. However, they may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. As FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives

[123] See, for example, Michael Wills, "Changes at Duke Energy Substations Crack Down on Copper Thieves," *WUNC Radio 91.5*, May 22, 2013; Scott Kraus, "Hit Hard by Copper Wire Thieves, PPL Fights Back," *The Morning Call* (Lehigh, PA), June 6, 2013.

[124] Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid overall uniformly reflect terrorism risk from a national perspective.

Quality of Federal Threat Information

The power industry's physical security risk assessments rely upon information about security threats provided by the federal government, among other sources, communicated through the ISAC, during DHS and other agency briefings, or through other channels. The quality of this threat information is a key determinant of what grid owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information—especially from the federal government—may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat. For example, prior to FERC's physical security order, the head of NERC, which initially opposed mandatory physical security standards stated,

> I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations.[125]

Differences in the interpretation or application of threat information, as discussed in the previous section, may be a reason why some large utilities have announced major new substation security initiatives while others have not.

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.[126] Threat information continues to be an uncertainty in the case of power grid physical security. For example, some federal officials reportedly have characterized the Metcalf incident as a domestic terrorist attack, potentially a "dry run" for a more destructive attack on multiple HV transformer substations, while the FBI has stated that it does not believe Metcalf was a terrorist incident.[127] Because the perpetrators have not been identified, it is impossible to know for certain, but the ambiguity has significant implications for HV substation security going forward. Although there is wide consensus that the Metcalf attack was extremely serious, some industry analysts have opined that FERC's physical security order may be an "overreaction" to Metcalf.[128] By contrast, former DHS Secretary Michael Chertoff has predicted that "the sophistication and resulting damage of the Metcalf attack will ... be exceeded" in a future attack.[129] Still others have expressed concern that FERC's physical security concerns

[125] Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Letter to Senate Majority Leader Harry Reid, February 12, 2014, p. 2, http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf.

[126] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

[127] Rebecca Smith, February 5, 2014.

[128] Deborah Carpentier, "NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance," *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, http://www.crowell.com/files/NERC-Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf.

[129] Michael Chertoff, "Building a Resilient Power Grid," *Electric Perspectives*, May/June 2014, p. 35.

may be too heavily focused on another Metcalf-type scenario (the last threat) rather than a wider range of potential future threats (the next threat).[130]

There is widespread agreement among government, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks would require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true vulnerability of the grid to a multi-HV transformer attack remains an open question. As Congress seeks to establish the best policies to address HV transformer vulnerability relative to other infrastructure security priorities, understanding this vulnerability in the context of specific demonstrable threats may become increasingly important. To this end Congress may examine how federal threat information is developed and used by grid owners, and how limitations and uncertainty of this information may affect the HV transformer physical security among electric utilities.

Recovery from HV Transformer Attacks

Physical security for HV transformer substations has the primary purpose of preventing successful attacks against these critical assets within the power grid. However, in the event of a successful attack, measures to minimize its effect on the overall grid are equally important so that the loss of any particular transformer remains a local event. To this end the electric power industry emphasizes its strategy of "defense-in-depth," which includes incident response and recovery in addition to preparation and prevention.[131] Industry initiatives to enhance grid resiliency, including incident recovery programs such as the DHS recovery transformer program and EEI's spare transformer program, contribute to the power grid's ability to sustain a terrorist attack without widespread grid failure. Indeed, some analysts have pointed to the Metcalf incident as a successful demonstration of grid resiliency; electric service was not interrupted despite the loss of a critical substation in the San Francisco Bay area. As Congress continues its examination of physical security policy, maintaining a holistic perspective on prevention and recovery as integrated aspects of HV transformer security may help to clarify an effective balance in terms of industry investment and regulatory oversight.

Author Contact Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030

[130] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

[131] Edison Electric Institute, "The Electric Power Industry's Commitment to Protecting Its Critical Infrastructure," February 2014, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Critical_Infra_Physical_Protection.pdf.

From: [redacted]
Sent: Monday, July 28, 2014 4:20 PM
To: ER-2.3; ER-2.4; Cynthia Pointer; [redacted] Joseph McClelland; [redacted]; Edward Franks; [redacted]
Subject: FW: Congressional Research Service: Physical Security of the US Power Grid
Attachments: CongResearchSvc Report_Physical-Security-of-the-U.S.-Power-Grid_June2014.pdf

Ross Johnson (below) is the new CIPC physical security subcommittee chair; very impressive background, eminently qualified, a personable leader who people are willing to follow. I take him to be an earnest, no excuses, 'do the right thing' individual – and from Edmonton, Alberta...

I've attached the report found at the link below.

[redacted]

From: Ross Johnson [mailto:rjohnson@capitalpower.com]
Sent: Monday, July 28, 2014 3:25 PM
To: psrg
Subject: Congressional Research Service: Physical Security of the US Power Grid

All,

This link will take you to an interesting report from the Congressional Research Service titled: Physical Security of the US Power Grid: High-Voltage Transformer Substations. The report is thirty pages long, and well worth the read, covering the importance of high-voltage transformers, physical security options available, and ongoing and future methods of protection. It also discusses CIP-014-1, and the NERC Spare Equipment Database, amongst other initiatives.

Many thanks to Allan Wick of Tri-State for passing it on.

http://www.rtoinsider.com/wp-content/uploads/CRS-Report-Physical-Security-of-the-U.S.-Power-Grid.pdf

Best regards,
Ross

Ross Johnson, CPP
Senior Manager, Security & Contingency Planning
Capital Power Corporation
10th Floor, EPCOR Tower
1200-10423 101 Street NW
Edmonton, Alberta
Canada T5H 0E9

Office +1 (780) 392-5482
[redacted]

non-responsive pages not provided

From: Christy Walsh
Sent: Wednesday, June 04, 2014 6:31 PM
To: David Morenoff; Maria Farinella; Martin Kirkwood; Michael McLaughlin (OEMR); Anna Cochrane; Jamie Simler; Jeff Wright; Ann Miles; Norman Bay; Larry Gasteiger; Michael Bardee; Edward Franks; Joseph McClelland; David Andrejcak; Lawrence Greenfield; Deborah Leahy; Shaheda Sultan; Roshini Thayaparan; Jacqueline Holmes; John Katz
Subject: Final QFRs
Attachments: LaFleur Transmittal and QFR Responses (6-4-14).pdf; FERC BAY QUESTIONS (Final).pdf

Senior Staff,
As requested by many of you, please find attached the final QFRs for both nominees that were provided to the committee this evening.
Thank you,
Christy

35 K

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

June 4, 2014

The Honorable Mary Landrieu
Chair
Committee on Energy and Natural Resources
United States Senate
Washington, DC 20510

Dear Chair Landrieu:

Thank you for the opportunity to testify before the Committee on Energy and Natural Resources on May 20, 2014 on my nomination to the Federal Energy Regulatory Commission.

Attached are my responses to questions for the record posed by the members of the Committee. Please let me know if I can be of further assistance.

Sincerely,

Cheryl A. LaFleur
Acting Chairman

Attachment

QUESTIONS FOR THE RECORD
FOR
MS. CHERYL LaFLEUR

SENATOR MARY LANDRIEU

Louisiana is at the center of America's energy revolution and issues before FERC affect Louisianans in many different ways.

I understand that both Commissioner LaFleur and Mr. Bay cannot answer questions about disputed issues pending before the Commission due to *ex parte* rules, but I would like remind you both of a number of issues that I have previously raised with FERC. These are by no means a comprehensive list of my concerns that impact Louisiana directly.

Question 1. TOLEDO BEND

Last weekend, I held a field hearing in Louisiana at the beautiful Toledo Bend Reservoir to discuss how the hydroelectric project there can further enhance the economic benefits it brings to the region.

The Toledo Bend dam and reservoir provide significant benefits to Northwest Louisiana through the abundant supply of clean water, renewable electricity, and recreation opportunities. The ongoing FERC relicensing process, however, threatens the economic promise of the project. The Sabine River Authority has already spent $10 million over the past 7 years on relicensing, a huge sum of money that could have otherwise been invested in new infrastructure needed to secure additional economic development and create jobs.

FERC can partially offset these costs by granting the Toledo Bend Project a new 50-year term as I requested in a letter I sent on February 5. Without objection, a copy of this letter will be entered into the Committee record of this hearing.

The problems Toledo Bend has faced over the past several years are not unique. **What is FERC doing to simplify the relicensing process and how it is making sure that the costs associated with relicensing aren't diminishing the economic benefits of hydroelectric projects like Toledo Bend?**

Answer: The Federal Power Act requires the Commission to ensure that hydropower licenses are best adapted to a comprehensive plan for developing affected waterways, which the Supreme Court has held requires an examination of all public interest considerations. In order to provide sufficient information for the Commission to understand the environmental impacts of relicensing a project, license applicants must provide the Commission information regarding affected resources. The costs of gathering this information will vary, depending on the complexity of the issues and the extent to which there is already existing information available.

above, if confirmed, I will continue to look for opportunities to remove barriers to interconnection of new resources while ensuring that all generators receive just and reasonable prices for their power.

Question 6. The attacks on the Metcalf substation have shown that physical security of the electric grid is a critical problem. As you know, I wrote to FERC on this issue, and you responded by tasking the North American Electric Reliability Corporation (NERC) to develop a national reliability standard. Should NERC also provide input on an approach for maintaining spare transformers that can be moved around the country as circumstances require?

Answer: I agree that the adequacy of transformer supply is important to the resiliency of the electric grid. In addressing supply chain and appropriate inventory levels, it is important to have a clear understanding of which assets are the most critical in terms of how their loss would impact operation of the bulk power system. The version of cybersecurity reliability standards recently approved by FERC (CIP version 5) expressly requires utilities to determine the criticality of cyber assets and tailor protections accordingly. The FERC directive that NERC develop a physical security standard also requires identification of the most critical facilities. In addition, FERC's final rule on geomagnetic disturbance standards also required identification of the assets most important to protect and explicitly identified inventory management as a possible mitigation strategy to be used under the standards.

NERC's petition to approve a physical security standard was filed with the Commission for review on May 23, 2014. It would be inappropriate for me to judge the merits before interested parties have an opportunity to submit comments to the Commission, so that we can consider all relevant arguments. I assure you that I will carefully consider the proposal and all filed comments to ensure that NERC's filing does adequately protect the public.

I also note that the Edison Electric Institute (EEI) has undertaken the voluntary Spare Transformer Program (STEP) and that NERC maintains the Spare Equipment Database (SED) Program. These programs are designed to help utilities identify and share spare transformers in emergencies. Finally, the Department of Homeland Security, the Department of Energy, and others are working to develop the Recovery Transformer (RecX), a prototype extra-high voltage (EHV) transformer that would significantly reduce the recovery time associated with EHV transformers. This initiative may play an important role in improving our ability to recover if a number of transformers are damaged concurrently for any reason.

Question 7. This reliability standard is intended to help safeguard the grid against attacks by humans. Do you believe that this standard would also provide adequate protection against extreme weather events?

Answer: As mentioned above, NERC's petition to approve a physical security standard was filed with the Commission for review on May 23, 2014. Because the reliability standard is pending before the Commission, I cannot comment on it at this time. I note that many other existing reliability standards are intended to mitigate the type of system impacts that may be caused by an extreme weather event.

SENATOR DEAN HELLER

Question on Order No. 1000:

Mr. Bay and Ms. LaFleur,

Order No. 1000 creates obligations for neighboring transmission planning regions to develop procedures for joint identification and evaluation of regional and interregional transmission needs, potential facilities to address those needs, and a cost allocation methodology for allocating the costs of such facilities. The costs of regional and interregional transmission facilities are expected to be allocated to customers roughly commensurate to the benefits they receive. FERC gave the industry some flexibility to comply with very broad directives. It is my understanding that the compliance process has been messy, and getting the requirements of the order into effect has been a significant challenge that has consumed FERC's time and policy attention for over a year and counting.

1. In your view, how much flexibility and deference, if any, should FERC provide individual planning regions to develop and implement unique methods for allocating costs to the recipients of the benefits? Do you think FERC should mandate certain aspects of compliance for sensitive issues such as binding cost allocation, or simply defer to each region's direction?

Answer: I believe that FERC's cost allocation policies should be flexible to meet regional needs in both established regional transmission organizations and in bilateral market regions. That is why I supported the regional transmission planning and cost allocation approach of Order No. 1000, which adopted minimum requirements for regional transmission planning and cost allocation, but gave regions flexibility to develop specific proposals that will meet regional needs and reflect regional differences. In evaluating filings submitted in compliance with Order No. 1000, we have not mandated a "one-size-fits-all" approach. Indeed, we have approved a variety of cost allocation proposals that satisfy the minimum requirements established in Order No. 1000.

Because the issue of binding cost allocation is pending before the Commission, I cannot comment on it at this time.

2. As you know, the West has a predominance of non-jurisdictional transmission providers compared to other regions. Given their significant footprint and unique compliance status on one hand and the need for enhanced operational coordination and planning across the region on the other, how should FERC balance these factors in seeking to facilitate broad utility participation, on a comparable and non-discriminatory basis, in the regional and interregional planning processes formed under the order?

Answer: I recognize the significant contributions of non-public utility transmission providers to regional transmission planning, and in Order No. 1000, the Commission encouraged their participation, noting that the success of the reforms called for in the rule would be enhanced if all transmission owners, including non-public utility transmission providers, participate. In

QUESTIONS FOR THE RECORD
FOR
Mr. Norman Bay

SENATOR MARY LANDRIEU

Louisiana is at the center of America's energy revolution and issues before FERC affect Louisianans in many different ways.

I understand that both Commissioner LaFleur and Mr. Bay cannot answer questions about disputed issues pending before the Commission due to *ex parte* rules, but I would like remind you both of a number of issues that I have previously raised with FERC. These are by no means a comprehensive list of my concerns that impact Louisiana directly.

Question 1. TOLEDO BEND

Last weekend, I held a field hearing in Louisiana at the beautiful Toledo Bend Reservoir to discuss how the hydroelectric project there can further enhance the economic benefits it brings to the region.

The Toledo Bend dam and reservoir provide significant benefits to Northwest Louisiana through the abundant supply of clean water, renewable electricity, and recreation opportunities. The ongoing FERC relicensing process, however, threatens the economic promise of the project. The Sabine River Authority has already spent $10 million over the past 7 years on relicensing, a huge sum of money that could have otherwise been invested in new infrastructure needed to secure additional economic development and create jobs.

FERC can partially offset these costs by granting the Toledo Bend Project a new 50-year term as I requested in a letter I sent on February 5. Without objection, a copy of this letter will be entered into the Committee record of this hearing.

The problems Toledo Bend has faced over the past several years are not unique. **What is FERC doing to simplify the relicensing process and how it is making sure that the costs associated with relicensing aren't diminishing the economic benefits of hydroelectric projects like Toledo Bend?**

Answer: The Supreme Court has held that the Federal Power Act requires the Commission to examine all public interest considerations to ensure that hydropower licenses are best suited to a comprehensive plan for developing affected waterways. License applicants must provide the Commission information regarding affected resources for the Commission to understand the environmental impacts of relicensing a project. Depending on the complexity of the issues involved in the licensing proceeding and the availability of existing information, the costs of gathering this information will vary. Further, there are other federal and state resource agencies involved in the licensing process, and if these agencies seek substantial new information the proceedings may be prolonged. My understanding is that within these constraints, the Commission makes every effort to ensure that hydropower relicensing proceedings are as

Question 10: We hear that base load energy is essential to the grid but struggles in organized markets. Can you describe benefits to the grid that base load power is uniquely positioned to provide?

Answer: Base load generators have traditionally been a source of dependability, fuel security, and resource diversity.

Question 11: Do you believe that base load energy resources are essential to the reliable operation of the grid?

Answer: Yes, I believe that base load energy resources are essential to the reliable operation of the grid. As described in response to Question 10, base load energy resources are a dependable source of generation that can also provide fuel security.

Question 12: What direction were you given by former Chairman Wellinghoff in your enforcement efforts?

Answer: As the Director of the Office of Enforcement (OE), I was responsible for implementing the enforcement program consistent with the Commission's Strategic Plan. Under the Strategic Plan, FERC's mission was to provide "reliable, efficient, and sustainable energy for consumers." There were two overall goals: (1) "just and reasonable rates, terms and conditions;" and (2) "infrastructure." OE effectuated both goals. Under the first goal, OE helped foster a "culture of compliance" among jurisdictional entities and used "risk-based audits." Under the second goal, OE helped "monitor, audit and enforce Reliability Standards." One priority for the Commission has been to ensure that consumers are protected from fraud and market manipulation and that there is a level playing field for all market participants.

Question 13: Have you had any contacts with former Chairman Wellinghoff since you were nominated to serve as Chairman?

Answer: No, I have not had any contacts with former Chairman Wellinghoff since I was nominated.

Question 14: If so, could you describe those contacts for the committee?

Answer: See response to Question 13.

Question 15: Why shouldn't FERC treat any net metering sale as a wholesale sale?

Question 16: If a utility's grid operating costs are being shifted from net metering customers to other customers, is that just and reasonable?

Answer: FERC, EPA, and DOE have communicated often regarding the potential reliability impacts of EPA's power sector regulations and have a joint staff document that describes how the agencies will monitor the power sector's progress in responding to certain EPA regulations affecting the electric power sector. The agencies should continue this effort to ensure that EPA is aware of any potential impacts its regulations may have on the reliability of the bulk-power system. The agencies also have adopted a more formal and transparent process regarding the issue of "fifth-year" extensions of compliance obligations under EPA's rules on power sector emissions of mercury and air toxics. Under this process, EPA has stated its intent to consider input from FERC and others on such requests, and FERC has issued a policy statement describing its process for voting on and communicating its recommendations to EPA. If confirmed, I am committed to working closely with the EPA and ensuring that reliability remains a priority at FERC.

Question 3. If confirmed as Chair, how would you ensure that EPA considers reliability issues going forward?

Answer: When EPA proposes new regulations, the Commission should carefully review the proposals and engage with a range of entities, including state officials, NERC, RTOs/ISOs, and industry. Adequate planning can help anticipate and address any potential implications for resource adequacy and reliability. If confirmed, I believe that FERC must continue to work closely with the EPA throughout this process. I recognize that EPA has responsibilities under the Clean Air Act and other legislation, but the Commission has a similar, and no less important, responsibility to help maintain the reliability of the bulk-power system. The key is open communication and a strong working relationship.

Question 4. In your testimony, you mentioned that you would have to recuse yourself from 43 enforcement matters currently pending before the Commission. How many total matters, enforcement and otherwise, are currently pending before FERC right now?

Answer: At the time of my hearing, there were 43 pending investigations in the Office of Enforcement. Under the most expansive potential application of the ethics rules, this appears to be the largest set of proceedings from which I could possibly need to recuse myself, if confirmed.

There are approximately 5,253 matters currently pending before the Commission. This number consist of all matters that are pending Commission action in every area of the agency, including Energy Projects, Electric Reliability, Policy and Innovation, Energy Market Regulation, matters before the General Counsel, and Enforcement matters.

Accordingly, when accounting for the entire body of pending matters before FERC, even taking the broadest approach to recusals, I would only potentially be recused from approximately 0.8 percent (less than 1 percent) of the matters pending before the Commission.

needed it. However, the Cochin pipeline, which has been transporting a very substantial amount of propane from Canada to the Midwest, is being repurposed to send other petroleum products in the opposite direction. Should FERC be given additional authorities to conduct a public interest determination before permitting the reversal of pipelines such as Cochin?

Answer: The Interstate Commerce Act (ICA) generally provides the Commission with jurisdiction only over the terms and conditions of tariffs of oil and product pipelines, including pipelines which ship propane and the rates the pipelines charge for those shipments. The Commission does not have jurisdiction over the entry, exit, ownership, construction or abandonment of oil and product pipelines because in the ICA, Congress determined oil and product pipelines should function as common carriers. As such, the decision to reverse the Cochin pipeline was a company business decision made in response to changing market conditions, outside the jurisdiction of the Commission. Given that the Commission has only used its emergency authority under the ICA once to address the propane situation this past winter, I believe it is worth evaluating FERC's existing authority before recommending that new authority be added. However, if I am confirmed, FERC staff would continue to monitor the propane markets. Further, I would ensure that FERC faithfully executes any additional jurisdiction given to it by Congress.

Question 4. Another issue during the propane shortage this past winter was that some pipeline terminals had long lines of truck drivers waiting to pick up loads of propane, while other terminals had no lines because truck drivers didn't know that propane was available there. Do you think it would be a good idea for FERC to improve transparency into pipeline operations so that we avoid this kind of confusion in the future?

Answer: Improving transparency into propane pipeline operations would be positive. The Commission does not currently have the authority under the Interstate Commerce Act to require propane pipelines to post operational flows or to require terminal operators to post propane supply information.

Question 5. Utilities installing wind turbines are often exempt from local zoning laws and can install 100-foot structures at will, but homeowners and businesses are subject to 35-foot or other height restrictions. What actions could FERC take to help homeowners and businesses who wish to install distributed generation projects such as community wind?

Answer: The Commission does not have jurisdiction over the installation of distributed generation projects such as community wind.

Question 6. The attacks on the Metcalf substation have shown that physical security of the electric grid is a critical problem. As you know, I wrote to FERC on this issue, and you responded by tasking the North American Electric Reliability Corporation (NERC) to develop a national reliability standard. Should NERC also provide input on an approach for

maintaining spare transformers that can be moved around the country as circumstances require?

Answer: The industry, through such efforts as the Edison Electric Institute's (EEI's) Spare Transformer Equipment Program, has been working to improve the ability of transformer owners to share spare transformers in the event of an attack. NERC also maintains an inventory list of spare transformers. In addition, over the last several years, the Department of Homeland Security and the Department of Energy have worked with the electric industry and a transformer manufacturer to design, build and demonstrate a "recovery transformer," which has undergone an encouraging operational test. The recovery transformer was designed to facilitate the quick transportation and installation that is so important when it is needed to restore service or reliability. If confirmed, I look forward to discussing these efforts with DOE, DHS, NERC, EEI, RTOs/ISOs, and other stakeholders.

Question 7. This reliability standard is intended to help safeguard the grid against attacks by humans. Do you believe that this standard would also provide adequate protection against extreme weather events?

Answer: In the proposed physical security standard, protection of identified substations may include resiliency or security measures. An example of a resiliency measure is the installation of a new substation that would make the electric grid less vulnerable to the loss of any one substation. It is premature for me to form a final opinion on this question. If confirmed, I would consider the proposed standard, which was filed with the Commission on May 23, 2014. Before forming my final opinion on the standard, I would consider the information contained in NERC's filing material and the public comments submitted to the Commission on the filing.

In addition, a wide range of current reliability standards are useful in protecting against the results of weather events, such as the transmission planning standards and the emergency preparedness and operations standards.

SENATOR JAMES E. RISCH

1. FERC took unprecedented action and sued the Idaho Public Utility Commission under Section 210(h) of the Public Utility Regulatory Policies Act (PURPA) in federal court. Although this case has been resolved, I am concerned about FERC taking similar action with states in the future. How do you believe FERC should interact with states? What do you believe the relationship between FERC and state regulators should be?

Answer: Because both FERC and state regulators are charged with protecting the public interest, they share a common interest and responsibility. It is important for FERC and state regulators to have a cooperative relationship while respecting each other's' jurisdiction. If confirmed, I look forward to working with my state colleagues, including through coordination with the National Association of Regulatory Utility Commissioners (NARUC).

From: Robert Ivanauskas <robert.ivanauskas@ferc.gov>
Sent: Thursday, June 26, 2014 12:08 PM
To: Joseph McClelland; David Andrejcak; Edward Franks; Michael Bardee; David Morenoff; Christy Walsh
Subject: FW: fyi
Attachments: CRS PhysSec HVTs 17Jun2014.pdf

Since I received this from a member of the general public, then it is already public. Thus, I am forwarding it to you so that you know what the public is reading on this topic.

From: Sabrina Campbell [mailto:svcampbell@aep.com]
Sent: Tuesday, June 24, 2014 2:05 PM
To: robert.ivanauskas@ferc.gov
Subject: fyi